ՀԱՄԱՑԱՆՑԻ ԿԱՌԱՎԱՐՈՒՄ

Յովան Կուրբալիա

4-րդ հրատարակություն

Այս գիրքը բավականին երկար պատմություն ունի: Առաջին հոդվածներն ու ընդհանուր մոտեցումը՝ ներառյալ «հինգ զամբյուղի» մեթոդաբանությունը, մշակվել էին 1997թ., Բրիտանական համագործակցության երկրների պետական գերատեսչությունների պաշտոնյաների համար տեղեկատվական-հաղորդակցության տեխնոլոգիաների (ՏՀՏ) բնագավառում քաղաքականության վերաբերյալ կրթական դասընթացներ նախապատրաստելու ընթացքում:

2004 թ. Diplo-ն առաջին անգամ հրատարակեց համացանցի կառավարման մասին իր նյութերից կազմված գիրքը, որը վերնագրված էր՝ «Համացանցի կառավարում. հիմնախնդիրներ, դերակատարներ, խոչընդոտներ»: Գրքի համահեղինակներն են՝ Ստեֆանո Բալդին, Էդուարդո Գելբշթայնը և Յովան Կուրբալիան: Այն դարձել է Diplo-ի հրատարակած «Տեղեկատվական հասարակության գրադարանի» մի մասնիկը: Առանձնահատուկ երախտագիտություն ենք հայտնում Էդուարդո Գելբշթայնին, ով մեծ ավանդ է ներդրել կիբեռանվտանգության, փոստաղբի և մասնավոր կյանքի անձեռնմխելիության բաժինների ստեղծման գործում: Շնորհակալ գործ են կատարել նաև Վլադիմիր Ռադունովիչը և Ջինջեր Փակը, ովքեր թարմացրել են դասընթացների նյութերը: Հեղինակների մյուս գործընկերների մեկնաբանություններն ու առաջարկությունները նշված են ըստ տեքստի: Այս գրքի պատկերազարդման մշակմանն իրենց գաղափարներով մեծապես օգնել են Ստեֆանո Բալդին, Էդուարդո Գելբշթայնը և Վլադիմիր Ռադունովիչը:

Հնդկաստանի Հայդերաբադ քաղաքում անցկացվող Համացանցի կառավարմանը նվիրված համաժողովի կապակցությամբ, NIXI-ի հետ Հնդկաստանի համագործակցությամբ 2008 -ին հրատարակվեց գրքի վերանայված տարբերակը՝ «Համացանցի կառավարում. Ներածություն» վերնագրով:

2009 թվականին վերանայված երրորդ հրատարակությունը լույս է տեսել Եգիպտոսի տեղեկատվական և հաղորդակցման տեխնոլոգիաների նախարարության հետ համագործակցությամբ: Այնուհետև «Համացանցի կառավարում» գրքի չորրորդ հրատարակությունը (2010 թ.) լույս է տեսել Ասիայի, Կարիբյան կղզիների և Խաղաղ Օվկիանոսյան երկրների տնտեսական համագործակցության խմբի քարտուղարության և Եվրամիության աջակցությամբ:

ՀԱՄԱՑԱՆՑԻ ԿԱՌԱՎԱՐՈՒՄ

Յովան Կուրբալիա

4-րդ հրատարակություն

Համացանցի ազդեցության շնորհիվ հասարակության սոցիալական, տնտեսական ու քաղաքական ավելի ու ավելի աճող տեղեկացվածությունը բազմապատկել է նրա կառավարման (Internet Governance) հարցի հանդեպ ուշադրությունը:

Գործող անձանցից ովքե՞ր կարող են ազդեցություն ունենալ համացանցի զարգացման վրա: Ինչ՞ քաղաքականություն են վարելու նրանք ցանցի բովանդակության, հասանելիության ապահովման, առևտրի, ֆինանսավորման, անվտանգության և համացանցի զարգացման համար կարևորագույն այլ հարցերի առնչությամբ: Սրանք ընդամենը մի քանի կարևոր հարցեր են, որոնց պատասխանները անհրաժեշտ է փնտրել համացանցի կառավարման շրջանակներում:

Հայաստանում առաջին անգամ հրատարկավող այս գիրքը Համացանցի Կառավարման (Internet Governance) յուրահատուկ տեղեկատու է:

DiploFoundation հիմնադրամի տնօրեն Յովան Կուրբալիայի գրքում ներկայացված են համացանցի կառավարման տեխնիկական, տնտեսական ու սոցիալ-մշակութային ասպեկտներն ու զարգացման հեռանկարները:

Համացանցի արդյունավետ կառավարումը հնարավոր է միայն պետական կազմակերպությունների, բիզնես համայնքի և քաղաքացիական հասարակության ակտիվ և կառուցողական փոխգործակցության շնորհիվ: Եվ պատահական չէ, որ այս գրքի բովանդակության և մոտեցումների վրա հիմնված ուսումնական ծրագրով 1997թ.-ից ի վեր Դիպլո Հիմնադրամում ավելի քան 1 000 դիվանագետներ, պետական ծառայողներ, ոչ կառավարական կազմակերպությունների աշխատակիցներ և ՏՀՏ մասնագետներ են վերապատրաստվել:

ՀԱՄԱՑԱՆՑԻ ԿԱՌԱՎԱՐՈՒՄ / Յովան Կուրբալիա - Երևան, Նոյյան Տապան, 2012, 226 էջ:

Published by DiploFoundation (2010)
Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta
Switzerland: DiploFoundation
Rue de Lausanne 56
CH-1202 Genève 21, Switzerland
E-mail: diplo@diplomacy.edu
Վեբ կայք http://www.diplomacy.edu

ISBN: 978-99932-53-23-5

Բովանդակություն

Առաջաբան

Երբ 2004թ. ընկերներիս պատմեցի, թե ինչով եմ զբաղվում WGIG–ում (Համացանցի կառավարման աշխատանքային խումբ), նրանք արդեն ինձ էին դիմում տպիչների վերանորոգման կամ ծրագրաշարերի տեղադրման խնդրանքներով:
Նրանք կարծում էին, որ ես զբաղված եմ համակարգիչներով: WGIG-ի իմ գործընկերների շրջանում փոքրիկ հարցում անցկացրեցի, թե ինչպես են նրանք մտերիմներին, գործընկերներին կամ երեխաներին բացատրում իրենց գործառույթները: Նրանք էլ իմ նման դժվարություններ էին ունեցել: Սա է պատճառներից մեկը, թե ինչու առաջացավ Դիպլո-ի դասագրքի և համացանցի կառավարման նկարների ստեղծման մտահղացումը:
Ընդամենը վեց տարի անց, նույն մարդիկ, ովքեր նախկինում խնդրում էին կամակարգիչը կարգաբերել, արդեն հարցնում ինձ, թե ինչպես պաշտպանել իրենց մասնավոր կյանքը ֆեյսբուքում կամ ինչպես ապահովել իրենց երեխաների ապահով և անվտանգ աշխատանքը Համացանցում: Ոմանք նույնիսկ հարցնում էին, արդյո՞ք ակնհայտ հանցավոր հարաբերությունները Չինաստանի և Google-ի միջև, կամ հաճախակի քննարկվող կիբեռպատերազմները կապ ունեն Համացանցի կառավարման հետ:
Ինչ առաջնթաց ենք մենք ապրել: Համացանցի կառավարումը ավելի ու ավելի հանրային է դառնում: Ժամանակակից հասարակությունը որքան ավելի է կախված Համացանցից, այնքան ավելի պահանջված է դառնում Համացանցի կառավարումը:
Համացանցի կառավարումը վերաբերում է բոլորիս, անկախ նրանից, մենք Համացանցի 2 միլիարդ օգտվողներից մեկն ենք, թե ոչ, քանի որ չօգտվողները նույնպես կախված են Համացանցի ծառայություններից:
Համացանցի կառավարումը ավելի շատ է առընչվում նրանց, ովքեր մերձեցել են էլեկտրոնային աշխարհին՝ էլեկտրոնային բիզնեսի կամ պարզապես ֆեյսբուքի միջոցով: Այնուամենայնիվ այն վերաբերում է պետական պաշտոնյաներին, զինծառայողներին, իրավաբաններին, դիվանագետներին՝ բոլոր նրանց, ով հանրային շահն է պաշտպանում կամ էլ հանրային կայունությունը. մասնավորապես պաշտպանում է մասնավոր կյանքի գաղտնիքը, մարդու իրավունքները, կամ էլ քաղաքացիական հասարակության և հասարակական աշխատանքի կիզակետում է գտնվում:
Վաղվա Google, Skype, Facebook, և Twitter ստեղծողները նավարկում են

ցանցում արդեն այսօր: Նրանց ստեղծագործությունը և նորարարությունը չպետք է արգելակել, այլ խրախուսել Համացանցի զարգացման նոր ավելի ստեղծագործ ուղիներ գտնելու համար: Համացանցի կառավարման հիմնական նպատակներից մեկը, զարգացման համար անհրաժեշտ և այնպիսի բարենպաստ իրավա-քաղաքական միջավայրի ստեղծումն է, որը թույլ կտա Համացանցը որպես զարգացման շարժիչ օգտագործել:
Հուսով եմ, որ այս գիրքը պարզ եւ մատչելի կերպով բացատրում է համացանցի կառավարման հիմնական գաղափարները: Ձեզանից ոմանք առաջին անգամ են բախվում այս առարկային: Մյուսների համար գիրքը պարզապես կօգնի վերհիշել այն ամենը, ինչ իրենք արդեն անում են իրենց բնագավառում՝ e-առողջապահություն, e-առևտուր, e-կառավարում, կամ մի այլ բնագավառում, որը Համացանցի կառավարման խնդիրների շարքում է:
Այս տարաբնույթ մոտեցման հիմքում ընկած է մի համեստ ցանկություն. իմ ներդրումն ունենալ աշխարհի միլիարդավոր մարդկանց համար Համացանցը ինտեգրված և բարենպաստ միջավայր պահպանելու գործում: Ի վերջո, հուսով եմ, ձեր ախորժակը կբացվի և գիքը կստիպի ձեզ ավելի խորը սուզվել այս սքանչելի և դինամիկ առարկայի մեջ:
Հետեւեք զարգացումներին http://www.diplomacy.edu/isl/ig/

Յովան Կուրբալիա
DiploFoundation

Բաժին 1

Ներածություն

Համացանցի կառավարումը հեշտ խնդիր չէ: Չնայած որ այն գործ ունի թվային աշխարհի գլխավոր խորհրդանիշի հետ, սակայն նրա հանդեպ կիրառելի չէ թվային (երկակի) տրամաբանությունը՝ «ճիշտ և սխալ»-ը կամ «լավ ու վատ»-ը: Այս հիմնախնդրի շրջանակներում գոյություն ունեցող պատկերացումների և իմաստների բազմաթիվ նրբություններն ու երանգներն անհրաժեշտություն են առաջացնում տարբերակների և փոխզիջումների մի ամբողջ շարք ենթադրող նմանատիպ մոտեցում կիրառել: Այդ պատճառով այս բրոշյուրի մեջ մենք չենք փորձում համացանցի կառավարման հարցի վերաբերյալ վերջնական եզրակացություններ կատարել: Այն նպատակ ունի այդ ոլորտում վերլուծությունների, բանավեճերի և արմատական հարցերի լուծման գործնական շրջանակներ առաջարկելու:

Ներածություն

Դամենամատաբար կարճ ժամանակում համացանցը դարձավ արդի հասարակության անբաժանելի մասը: Ներկայացնենք այսօր առկա համացանցի մի քանի բնութագրական գծեր (2009 թ. վերջ).

-որոշ գնահատականների համաձայն, ամբողջ աշխարհում 1,5 միլիարդ մարդ օգտվում է համացանցից.

-չափազանց կարևոր ազդեցություն է գործել կրթության, առողջապահության բնագավառներում, իշխանական մարմինների գործառույթների և այլ բնագավառներում գործունեություն ծավալող հասարակության վրա.

-կիբեռհանցագործություն, օրինակ՝ խարդախություն, անօրինական խաղեր և ֆիշինգ (անձնական տեղեկատվության անթույլատրելի օգտագործում և այն գողանալը).

-վնասաբեր կոդի և փոստաղբի ձևերով տեխնոլոգիաների անօրինական ու անպատշաճ օգտագործում:

Համացանցի ազդեցության շնորհիվ հասարակության սոցիալական, տնտեսական ու քաղաքական ավելի ու ավելի աճող տեղեկացվածությունը ակտիվացրեց համացանցի կառավարման հարցի հանդեպ ուշադրությունը: Համացանցի կարգավորումը անհրաժեշտ է, որպեսզի՝

-կանխվի կամ, ծայրահեղ դեպքում, նվազագույնի հասցվի համացանցի քայքայման ռիսկը, որի դեպքում համացանցը, հնարավոր է, մասնատվի մի քանի ցանցերի.

-պահպանվի համացանցի տեխնիկական համատեղելիությունը և բոլոր բաղադրամասերի փոխգործակցության կարողությունը.-գործունեություն ծավալող տարբեր անձանց իրավունքները պաշտպանվեն և որոշեն նրանց պատասխանատվության սահմանները.

- համացանցից օգտվողներին զերծ պահեն տեխնոլոգիաների անօրինական և անպատշաճ օգտագործման հետևանքներից.

-պաշտպանվեն հասարակական շահերը՝ պետական և գլոբալ մակարդակով.

-նպաստեն համացանցի հետագա զարգացմանը:

Տեխնոլոգիական զարգացման իրավական տեսակետների և սոցիալական հետևանքների վերլուծությունը անխուսափելիորեն հետ է մնում տեխնոլոգիական նորարարություններից: Դա վերաբերում է նաև համացանցին:

Համացանցի կարգավորման հարցերի վերաբերյալ միջազգային բանակցությունները մի քանի կարևորագույն փուլ են անցել, սակայն դեռևս չեն կարող ավարտված համարվել, նույնիսկ, հեռու են համացանցի կառավարման հարցում համաձայնության հասնելուց:
Գործող անձանցից ովքե՞ր կարող են ազդեցություն ունենալ համացանցի զարգացման վրա: Ի՞նչ քաղաքականություն են վարելու նրանք ցանցի հասանելիությունը ապահովելու, առևտրի, նյութերի բովանդակության (կոնտենտի), ֆինանսավորման, անվտանգության և այլ հարցերի առնչությամբ, որոնք համացանցի զարգացման համար համարվում են կարևորագույն: Սրանք ընդամենը մի քանի կարևոր հարցեր են, որոնց պատասխանները անհրաժեշտ է փնտրել համացանցի կառավարման շրջանակներում:
Համացանցն ու վիճակագրությունն այնքան էլ սերտ կապված չեն միմյանց: Համացանցի գոյության առաջին իսկ օրերից բարդ էր ստույգ որոշել օգտվողների և վեբկայքերի քանակը, միմյանց փոխանցվող տվյալների (թրաֆիկ) ծավալը, ֆինանսական ցուցանիշները և շատ այլ պարամետրեր: Ընդ որում, թվերը հաճախ օգտագործվում են համացանցի զարգացման ընթացքի շուրջ աղմուկ բարձրացնելու համար, ինչը դրանց հավաստիությունն ավելի նվազեցնում է:[1]

Ի՞նչ է նշանակում «համացանցի կառավարում» տերմինը

«Համացանց» տերմինն ինքնին վեճեր է առաջացնում, որոնք հետագայում շարունակվում են համացանցի կառավարման մասին վիճաբանություններում: Սա միայն լեզվաբանական բծախնդրության հարց չէ: Այս տերմինի իմաստային տարբեր երանգները քաղաքական ուղու մշակման տարբեր մոտեցումներ և սպասումներ են ծնում: Օրինակ՝ հեռահաղորդակցման ոլորտի մասնագետները համացանցի կառավարման հիմնախնդիրը դիտարկում են տեխնիկական ենթակառուցվածքի հատվածով:
Համակարգչային տեխնոլոգիաների բնագավառի մասնագետները հիմնականում ուշադրություն են դարձնում տարբեր ստանդարտների, լեզվի և ներդիրների մշակմանը, ինչպիսիք են, օրինակ՝ XML-ը կամ Java-ն:
Հեռահաղորդակցման մասնագետները շեշտադրում են տեղեկատվության փոխանակման պարզեցումը:
Մարդու իրավունքների համար պայքարող ակտիվիստները համացանցի կառավարումը դիտարկում են համոզմունքների ազատ արտահայտման, մասնավոր կյանքի գաղտնիության պահպանման և անձի այլ իրավունքների տեսանկյունից:
Իրավաբաններն ուշադրություն են դարձնում իրավասության և վեճերի լուծման հարցերին:
Ողջ աշխարհի քաղաքագետները, սովորաբար խոսում են զանգվածային լրատվամիջոցների և ընտրողների արձագանքին արժանացած հարցերի

մասին, օրինակ՝ հեռանկարների (որքան շատ համակարգիչ՝ այնքան լավ կրթություն) և սպառնալիքների (համացանցի անվտանգություն, երեխաների պաշտպանություն) մասին:
Դիվանագետներին, առաջին հերթին, անհանգստացնում է ազգային շահերի պաշտպանության և կարգավորման գործընթացը: Իրար հակասող մասնագիտական տեսակետների ցանկը, որ համացանցի կառավարմանն է հանձնված, կարելի է շարունակել:
Տեղեկատվական հասարակության 1 հարցերով համաշխարհային բարձր մակարդակի հանդիպման շրջանակներում առաջարկվել է համացանցի կառավարման հետևյալ սահմանումը. «Համացանցի կառավարումը համացանցի զարգացումն ու օգտագործումը կանոնակարգող կառավարությունների, մասնավոր սեկտորի և քաղաքացիական հասարակության՝ իրենց համապատասխան դերն իրականացնելիս, ընդհանուր սկզբունքների, նորմերի, կանոնների, ընդունած որոշումների ընթացակարգերի ու ծրագրերի մշակումն ու կիրառումն է »:[2]
Աշխատանքային այս սահմանումը բանավեճերի համար թեև ելակետային է, այնուամենայնիվ այն չի օգնում լուծել երկու կարևոր՝ «համացանց» և «կառավարում» տերմինների տարբեր մեկնաբանությունների հիմնախնդիրը:
Տեղեկատվական հասարակության հարցերով համաշխարհային գագաթաժողովը հրավիրվել էր ՄԱԿ-ի նախաձեռնությամբ և անց էր կացվել երկու փուլով՝ 2003 թ. Ժնևում և 2005 թ. Թունիսում:
Հեռահաղորդակցության միջազգային միությունը միջազգային կազմակերպություն է, որի շրջանակներում կառավարությունները և մասնավոր սեկտորը համակարգում են համաշխարհային ցանցերն ու էլեկտրոնային կապի ծառայությունները: Հեռահաղորդակցության միջազգային միությունը հիմնադրվել է Փարիզում, 1865 թ.՝ որպես Միջազգային հեռագրամիություն: Ներկա անվանումը միությունը ստացել է 1934 թ., իսկ 1947 թ. դարձել է ՄԱԿ-ի մասնագիտացված հիմնարկությունը:

Համացանց

Որոշ հեղինակներ պնդում են, որ «համացանց» հասկացությունը չի ընդգրկում թվային տեխնոլոգիաների զարգացման գոյություն ունեցող բոլոր տեսակետները: Սովորաբար՝ որպես առավել ամբողջական, առաջարկվում է երկու տերմին՝ «տեղեկատվական հասարակություն» և «տեղեկատվական հաղորդակցման տեխնոլոգիաներ»: Այս հասկացություններն ընդգրկում են այնպիսի ոլորտներ, որոնք անմիջականորեն համացանցի սահմաններից դուրս են, օրինակ՝ բջջային կապը: Սակայն «համացանց» տերմինի կիրառման օգտին է խոսում գլոբալ հաղորդակցման ուղիների արագընթաց անցումը համացանցին՝ որպես հիմնական տեխնիկական ստանդարտի: Ամենահաս համացանցը արագընթաց աճում է ոչ միայն քանակական առումով, այլև առաջարկվող ծառայությունների սպեկտրի տեսակետից, որոնցից ամենաաչքի ընկնողը համացանցի միջոցով ձայնային փոխանցման արձանագրումն է (VoIP), ինչն էլ կարող է փոխարինել սովորական հեռախոսային կապին:

Կառավարում

Համացանցի կառավարման հիմնախնդիրների մասին բանավեճերի, հատկապես 2003 թ. Ժնևում WSIS-ի (World Summit of the Information Society, տեղեկատվական հասարակության հարցերով համաշխարհային բարձր մակարդակի հանդիպում) առաջին փուլի ընթացքում հակասություններ առաջացրին «կառավարում» տերմինը և դրա տարբեր մեկնաբանությունները: Այդ մեկնաբանություններից մեկի համաձայն, «կառավարումը» կառավարություն բառի հոմանիշն է: Շատ պետությունների ներկայացուցիչներն ի սկզբանե այդ հասկացության մեջ այդպիսի իմաստ էին դրել և ենթադրում էին, որ պետությունները միջկառավարական հիմունքներով պետք է կանոնակարգեն համացանցը՝ այլոց, հիմնականում ոչ պետական դերակատարների սահմանափակ մասնակցությամբ:[3]

Այսպիսի մեկնաբանությանը հակադրվեց «կառավարում» տերմինի այլ, ավելի լայն ըմբռնումը, որը ենթադրում է տարբեր, այդ թվում՝ ոչ պետական ինստիտուտների գործունեության կարգավորում: Հենց այս գնահատականից կառչեցին համացանցային ընկերությունները, քանի որ դա ավելի է համապատասխանում համացանցի ստեղծման իսկ օրվանից նրա կարգավորման առանձնահատկություններին: Տերմինաբանական խառնաշփոթը կրկնապատկվեց *«կառավարում» (governance, անգլ.)* բառի այլ լեզուներով տարբեր թարգմանությունների շնորհիվ: Իսպաներենով այդ տերմինը գերազանցապես վերաբերում է պետական գործունեությանը կամ կառավարությանը *(gestion publica, gestion del sector publico, funcion de gobierno)*: Ֆրանսերենը նույնպես այդ բառն արտահայտում է պետական և կառավարության գործունեությունը *(gestion des aff aires publiques, effi cacite de l'administration, qualite de l'administration, mode de gouvernement)*: Նման իրավիճակ է նկատվում նաև պորտուգալերենում՝ ակնհայտ է այդ տերմինի կապը պետական սեկտորի և կառավարության գործունեության հետ *(gest o publica, administrac o publica)*:

Համացանցի կառավարման զարգացումը

Համացանցի կառավարման սկզբնական շրջան (1970-1994 թթ.)

Համացանցը նախապես սկսել է գործել որպես կառավարության նախագիծ: 1960-ական թվականների վերջին ԱՄՆ կառավարությունը ֆինանսավորում է DAPRA Net ցանցի զարգացումը, որը նախագծել էր պաշտպանության նախարարության հետազոտական հեռանկարային ծրագրերի վարչությունը՝ որպես հաղորդակցման հուսալի միջոց: 1970-ականներին, երբ ստեղծվեց TCP/IP արձանագրությունը, այդ ցանցը դարձավ այն, ինչը ներկայում կոչվում է համացանց: Համացանցի հիմնական սկզբունքներից մեկը նրա բաշխման բնույթն է. տվյալների փաթեթը կարող է ցանցում փոխանցվել տարբեր ուղղություններով՝ շրջանցելով ավանդական անջրպետները և

Համացանցը կամ համացանցն ու դիվանագիտության լեզուն

2003 թ. «The Economist» ամսագիրն առաջին անգամ «համացանց» բառը տպագրեց փոքրատառով: Խմբագրության այդ քաղաքականությունն այն փաստի վկայությունն էր, որ համացանցն արդեն դարձել էր առօրյա կյանքի մի մասնիկը, դադարել էր առանձնահատուկ նշանակության ինչ-որ բան լինելուց: Այդպիսով, համաշխարհային ցանցին ևս բաժին հասավ այն ճակատագիրը, ինչ որ շատ այլ գյուտերին, օրինակ՝ հեռագրին, հեռախոսին, ռադիոյին, հեռուստատեսությանը:
2006 թ. նոյեմբերին Անթալիայում տեղի ունեցած Էլեկտրոնային կապի միջազգային միության համաժողովի ընթացքում հարց ծագեց համացանց բառը գլխատառերով թե փոքրատառով գրելու մասին: Այդ հարցը քաղաքական մասշտաբի հարց դարձավ, երբ համաժողովում համացանցի կառավարման հարցերի մասին բանաձևում «Համացանց» բառը, ի տարբերություն ավանդական գրության ձևի, հայտնվեց փոքրատառով:
Այդ ժամանակ ԱՄՆ դեսպան Դևիդ Գրոսը, ով զբաղվում էր համացանցի կառավարման հիմնախնդիրներով, մտահոգություն հայտնեց այն մասին, որ փոքրատառով գրությունը կարող է վկայել Էլեկտրոնային կապի միջազգային միության այն մտադրության մասին, որ համացանցը կարող է դիտարկել հեռահաղորդակցման այլ համակարգերի հետ միևնույն շարքում: Որոշ անձինք դա մեկնաբանում էին որպես դիվանագիտական ազդակ այն մասին, որ Էլեկտրոնային կապի միջազգային միությունը ձգտում է ավելի նշանակալի դեր խաղալ համացանցի կառավարման գործում:[4]

վերահսկողության մեխանիզմները: Տեխնոլոգիական այս սկզբունքին համապատասխանում էր նախնական փուլերում համացանցի կարգավորմանը ցուցաբերվող նույնանման մոտեցումը: Այդպիսին էր 1986 թ. ստեղծված համացանցի նախագծման աշխատանքային խումբը (IETF)[3], որը կառավարում էր համացանցի հետագա զարգացումը՝ համագործակցության և համաձայնության հիման վրա որոշումներ ընդունելով ու մասնակիցների լայն շրջանակ ներգրավելով:
Համացանցը չի ունեցել կենտրոնական կառավարություն, կենտրոնացված ծրագիր, «մեծ ռազմավարություն»: Այս ամենի արդյունքում հանրահայտ դարձավ այն պնդումը, որ համացանցը ձևավորում է եզակի մի ծավալ, որն այլընտրանքային է ժամանակակից աշխարհի քաղաքական համակարգին: Հանրահայտ «Կիբեռտարածությունների անկախության հռչակագրի» հեղինակ Ջոն Փերի Բարլոուն դիմում է բոլոր երկրների կառավարություններին, գրելով.
«Համացանցն իր բնույթով վերազգային է, դրանում կիրառելի չէ պետական ինքնավարության սկզբունքը և ձեր (պետական) ինքնավարությունը մեզ վրա չի տարածվում: Մենք՝ ինքներս պետք է որոշումներ ընդունենք».[4]

«DNS պատերազմ» (1994–1998)

Կարճ ժամանակում պետություններն ու բիզնեսը գիտակցեցին գլոբալ ցանցի կարևորությունը և համացանցի կառավարման հանդեպ ապակենտրոնացված մոտեցումը փոփոխությունների ենթարկվեց: ԱՄՆ Գիտության ազգային հիմնադրամը, որ ղեկավարում էր համացանցի կարևոր

ենթակառույցը, 1994 թ. որոշում է դոմենային անունների համակարգի ղեկավարումը հանձնել ԱՄՆ-ում գրանցված ենթակապալառու Network Solutions Inc (NSI) մասնավոր ընկերությանը: Համացանցային միությունը բացասաբար վերաբերվեց այդ քայլին, ինչն էլ առաջացրեց, այսպես կոչված, DNS պատերազմ: «DNS պատերազմը» համացանցի կարգավորման գործընթացի մեջ ներգրավեց նոր մասնակիցների՝ միջազգային կազմակերպությունների և պետությունների: Այն ավարտվեց 1998 թ., երբ ստեղծվեցին նոր կազմակերպություն՝ Համացանցում համարների և անունների շնորհման կորպորացիա (Internet Corporation for Assigned Names and Numbers, ICANN): Այդ ժամանակից սկսած համացանցի կառավարման հարցերի շուրջ բանավեճը բնորոշվում է կառավարությունների ավելի ակտիվ ներգրավմամբ:

Տեղեկատվական հասարակության հարցերով համաշխարհային բարձր մակարդակի հանդիպում (2003–2005)

2003 թ. Ժնևում և 2005 թ. Թունիսում անցկացված տեղեկատվական հասարակության հարցերով համաշխարհային բարձր մակարդակի հանդիպման ժամանակ համացանցի կառավարման մասին հարցը պաշտոնապես մտցվեց դիվանագիտական օրակարգ: WSIS-ի Ժնևյան փուլի մասնակիցները, որին նախորդել էին մի շարք նախապատրաստական կոմիտեների և տարածաշրջանային հանդիպումներ, առաջարկել էին քննարկել տեղեկատվության և հաղորդակցության հետ կապված հարցերի լայն շրջանակ: Բացի այդ, նախապատրաստական և տարածաշրջանային հանդիպումների ընթացքում նույնիսկ չեն հիշատակվել «համացանց» բառը և «համացանցային կառավարում» արտահայտությունը:[5] 2005 թ. հունվարին տեղի ունեցած Արևմտյան Ասիայի տարածաշրջանային հանդիպման ընթացքում համացանցի կառավարումը դարձավ WSIS բանակցային գործընթացի մի մասը, իսկ WSIS-ի Ժնևյան փուլի արդյունքների համաձայն, համացանցի կառավարումը դարձավ գագաթաժողովի ամենակարևոր հարցը: Ժնևում տեղի ունեցած հանդիպման մասնակիցները, երկար բանակցությունների և վերջին պահին կնքած համաձայնագրերի արդյունքում որոշում ընդունեցին համացանցի կառավարման հարցերի առնչությամբ ստեղծել աշխատանքային խումբ (Working Group on Internet governance, WGIG): WGIG-ը հաշվետվություն էր նախապատրաստել, որը հիմք ծառայեց 2005 թ. նոյեմբերին Թունիսում անցկացվող WSIS-ի երկրորդ փուլի շրջանակներում հետագա բանակցությունների համար: Հանդիպման հանրագումարային փաստաթուղթը, որ կոչվում էր «Ծրագիր տեղեկատվական հասարակության համար», մանրամասնորեն քննարկում է համացանցի կառավարման հիմնախնդիրը, ներառյալ այդ հասկացության սահմանումը, լուծում պահանջող ոլորտների ցանկը, ինչպես նաև ընդգրկում է համացանցի օգտագործման կառավարմանը վերաբերող հարցերի ֆորում (Internet Governance Forum, IGF) ստեղծելու մասին որոշում: Ֆորումը, որի առաջին

«Էլեկտրոնային», «վիրտուալ», «կիբեռ», «թվային» բառերը

«Էլեկտրոնային», «վիրտուալ», «կիբեռ», «թվային» ածականները կիրառվում են համացանցի և տեղեկատվական-հաղորդակցման տեխնոլոգիաների զարգացման տարբեր տեսակետները ներկայացնելու համար: Այս բառերի կիրառումն սկսվել է 1990-ականներից: Դրանք արտացոլում են տարբեր սոցիալական, տնտեսական և քաղաքական գործոններ, որոնք ազդում են համացանցի զարգացման վրա: Օրինակ՝ գիտական ընկերությունների ներկայացուցիչներն ու առաջին շահագործողները (համացանցի պիոներները) «կիբեռ», «թվային» բառերն օգտագործում էին, որպեսզի ընդգծեն «նոր հիասքանչ աշխարհ» ձևավորող համացանցի նորարարական բնույթը: «Էլեկտրոնային» բառի սահմանումը, որպես կանոն, զուգակցվում է էլեկտրոնային առևտրի (e-commerce) և 1990-ականների վերջին համացանցի առևտրայնացման հետ:

«Թվային» տերմինը հիմնականում գործածության մեջ է մտել տեխնոլոգիայի շրջանակներում և տարածում է գտել «թվային ճեղքման» մասին բանավեճերի համատեքստում:

«Կիբեռ» տերմինը առաջին անգամ միջազգային մակարդակով օգտագործվել է 2001թ. կիբեռհանցագործության մասին Եվրախորհրդի ընդունած համաձայնագրի մեջ: Ներկայում այն կիրառվում է կիբեռանվտանգության հիմնախնդիրները ներկայացնելիս: Այս բնագավառում Հեռահաղորդակցության միջազգային միության (ՀՄՄ) նախաձեռնությունը ստացել է «Կիբեռանվտանգությունը գլոբալ օրակարգային հարց» անվանումը:

«Վիրտուալ» տերմինը միջազգային փաստաթղթերում հազվադեպ է օգտագործվում:

«Էլեկտրոնային» ածականը առանձնահատուկ ժողովրդականություն է ձեռք բերել ԵՄ-ում: Այս բառի օգնությամբ էլեկտրոնային առողջապահության (e-health) կամ էլեկտրոնային գիտության բնագավառներում գրում են քաղաքական տարբեր նախաձեռնությունների մասին: WSIS շրջանակներում այս տերմինը առաջին անգամ կիրառվել է Բուխարեստում տեղի ունեցած Համաեվրոպական տարածաշրջանային հանդիպման ընթացքում, այնուհետև WSIS նյութերում և փաստաթղթերում դարձել է հիմնական օգտագործվող բառերից մեկը: WSIS որոշումներն իրականացվում են այնպիսի գործունեություններում, որոնք ընդգրկում են էլեկտրոնային կառավարություն, էլեկտրոնային գործ, էլեկտրոնային ուսուցում, էլեկտրոնային առողջություն և էլեկտրոնային համակարգով աշխատանքի տեղավորում, էլեկտրոնային գյուղատնտեսություն, էլեկտրոնային գիտություն (e-government, e-business, e-learning, e-health, e-employment, e-agriculture, e-science) ուղղությունները:

նիստը տեղի է ունեցել 2006 թ. հոկտեմբերին Աթենքում, համացանցի կառավարման հիմնախնդիրների միջազգային քննարկման նոր մոդել է: Այն բազմակողմանի ինստիտուտ է, որը գումարվում է ՄԱԿ-ի գլխավոր քարտուղարի որոշմամբ: Ֆորումի մանդատը վերանայվելու է հինգ տարի հետո:

2006թ. իրադարձությունները

2005 թ. նոյեմբերին Թունիսում տեղի ունեցած հանդիպման ավարտից հետո 2006 թ. համացանցի կառավարման հարցերով բանավեճերի առարկա դարձավ երեք կարևորագույն իրադարձություն: Առաջին՝ ԱՄՆ առևտրի նախարարության և ICANN-ի միջև փոխըմբռնման մասին հուշագրի գործողության ժամկետի ավարտն ու նորի ստորագրումը: Չարդարացան այն հույսերը, որ այդ իրադարձությունը կփոխի ԱՄՆ կառավարության և ICANN-ի փոխհարաբերությունների բնույթը ու վերջինս կդառնա նոր

տեսակի միջազգային կազմակերպություն: Հուշագրի նոր տարբերակն ընդամենը մի փոքր թուլացրեց ԱՄՆ կառավարության և ICANN-ի միջև կապը, որը գոյություն ուներ կազմակերպության ստեղծման պահից, թեև չէր բացառում հետագայում ICANN-ի վերջնականապես ինտերնացիոնալացման հավանականությունը:
2006 թ. երկրորդ իրադարձությունը Աթենքում անցկացվող համացանցի կառավարման հարցերի վերաբերյալ ֆորումն էր: Այն իր տեսակի մեջ առաջինն էր. շատ բաներում ֆորումն իրենից ներկայացնում էր բազմակողմ դիվանագիտության փորձարարական ձևաչափ: Ֆորումն իսկապես բազմակողմանի էր: Համացանցի կարգավորման գործընթացում ներգրավված բոլոր գործող անձինք՝ պետությունները, գործարար կառույցները և քաղաքացիական հասարակության ներկայացուցիչները, մասնակցում էին իրավահավասարության հիմունքներով: Սովորական չէր ֆորումի սեմինարների և հիմնական իրադարձությունների կազմակերպչական կառուցվածքը: Լրագրողները վերահսկում էին բոլոր քննարկումները, հետևաբար, ֆորումը տարբերվեց ՄԱԿ-ի ավանդական համաժողովների ձևաչափից: Սակայն քննադատները հայտարարեցին, որ ֆորումն ընդամենը «խոսելու տեղ է», որը չի տալիս հանրագումարային փաստաթղթերի կամ գործողությունների ծրագրերի ձև ունեցող իրական արդյունքներ:
Երրորդ կարևոր իրադարձությունը 2006 թ. նոյեմբերին Անթալիայում (Թուրքիա) տեղի ունեցած Հեռահաղորդակցության միջազգային միության (ՀՄՄ) լիազոր համաժողովն էր: Համաժողովում ՀՄՄ-ի նոր գլխավոր քարտուղար ընտրվեց դոկտոր Համադուն Տուրեն: Նա հայտարարեց, որ կազմակերպությունն ավելի մեծ ուշադրություն պետք է դարձնի կիբեռանվտանգության հիմնախնդիրներին և աջակցի զարգացմանը: Բոլորը սպասում էին, որ նրա ղեկավարությամբ կփոխվի նաև ՀՄՄ-ի մոտեցումը համացանցի կառավարման հանդեպ:

2007թ. իրադարձությունները

2007 թ. ICANN-ում բանավեճեր էին տեղի ունենում «մեծահասակների համար» «xxx» դոմեն ստեղծելու հավանականության շուրջ: Արդյունքում վերականգնվեցին համացանցի կառավարման շատ այլ հարցերի վերաբերյալ քննարկումները, ներառյալ ICANN-ի իրավասության ոլորտի հարցը, հատկապես այն, թե ICANN-ն արդյոք պետք է բացառապես տեխնիկական կարգավորմամբ զբաղվի, թե՞ նրա իրավասությունների մեջ են մտնում պետական քաղաքականության հարցեր: «xxx» դոմենի առնչությամբ ԱՄՆ-ի և այլ երկրների միջամտությունը սրում են ICANN-ի աշխատանքներում պետությունների մասնակցության հարցը: 2007 թ. նոյեմբերին Ռիո դե Ժանեյրոյում անցկացվող IGF երկրորդ հանդիպման ընթացքում գլխավոր իրադարձությունը դարձավ ֆորումի օրակարգում համացանցի չափազանց կարևոր ռեսուրսների մասին (անունների և հասցեների ծավալը) կետ մտցնելը:

2008թ. իրադարձությունները

2008 թ. կարևորագույն իրադարձությունը, որը շարունակելու է ազդեցություն ունենալ համացանցի կառավարման գործընթացի (ինչպես նաև քաղաքականության այլ ոլորտների) վրա, ԱՄՆ նախագահ Բարաք Օբամայի ընտրությունն էր: Նախագահական ընտրությունների ընթացքում նա լայնորեն օգտագործեց համացանցն ու Վեբ 2.0 տեխնոլոգիաները: Որոշ մարդիկ պնդում են, որ հենց համացանցն օգտագործելն էլ դարձավ Օբամայի հաջողություններից մեկը: Բ. Օբամայի խորհրդատուների շարքում էին համացանցային արդյունաբերության շատ ներկայացուցիչներ, ներառյալ Google ընկերության գլխավոր տնօրենը:

Բացի տեխնոլոգիական իրազեկվածությունից, նախագահ Օբամայի համար բնութագրական է միջազգային հիմնախնդիրները բազմակողմանիորեն լուծելու նրա մեծ հակումը, ինչն անխուսափելիորեն, ազդեցություն կունենա ICANN-ի ինտերնացիոնալացման և համացանցի կառավարման միջազգային գործունեության կարգ ձևավորելու մասին բանավեճերի վրա: 2008 թ. համացանցի կառավարման կարևորագույն հարցերից մեկը դարձավ, այսպես կոչված, ցանցային չեզոքությունը:[5] Այս հարցերի մասին նույնիսկ հիշատակվեցին նախընտրական պայքարում, ընդ որում, Բարաք Օբաման հանդես եկավ ի պաշտպանություն ցանցային չեզոքության սկզբունքի: Այս թեմայի շուրջ ԱՄՆ-ում բանավեճերը տեղի են ունենում երկու հակառակորդ խմբերի միջև: Ի պաշտպանություն ցանցային չեզոքության հանդես են գալիս, հիմնականում այսպես կոչված, համացանցային արդյունաբերության ներկայացուցիչները, այդ թվում այնպիսի ընկերություններ, ինչպիսիք են՝ Google-ը, Yahoo!-ն և Facebook –ը: Ցանցային չեզոքության սկզբունքը խախտելու արդյունքում համացանցի կառույցի փոփոխությունը կարող է նրանց բիզնեսը վտանգի ենթարկել: Հակառակ դիրքորոշում են գրավել հեռահաղորդակցության այնպիսի ընկերություններ, ինչպիսիք են՝ Verizon և AT&T, համացանցային ծառայություններ մատուցողներ (պրովայդերներ) և մուլտիմեդիական արդյունաբերության ներկայացուցիչներ: Մի շարք պատճառներով, բիզնեսի այս բնագավառի ներկայացուցիչները նախընտրում են որոշակի տարբերակում՝ ցանցով հաղորդվող տվյալների առնչությամբ: Մեկ այլ կարևորագույն իրադարձություն էր Facebook-ի և սոցիալական այլ ցանցերի արագ աճը: Համացանցի կառավարման ոլորտում Վեբ 2.0 գործիքների աճող հանրաճանաչությունը օրակարգում դնում է Facebook-ում և նմանատիպ ցանցերում մասնավոր կյանքի անձեռնմխելիության և տվյալների պաշտպանության հարցերը:

5. «Ցանցային չեզոքության» սկզբունքի համաձայն, տվյալները համացանցային ալիքներով պետք է փոխանցվեն առանց խտրականության, անկախ բովանդակության, ուղարկող անձի, ստացողի և այլն: Այդ սկզբունքի խախտում է համարվում, օրինակ՝ որպես նյութերի ավելի արագ բեռնման որոշ կայքերին հեռահաղորդակցության ընկերությունների կողմից առաջնություն տալը:

2009թ. իրադարձությունները

2009 թ. առաջին կեսին վաշինգտոնյան շրջանակների ներկայացուցիչները փորձում էին որոշել համացանցի վերաբերյալ ԱՄՆ նախագահ Բ. Օբամայի քաղաքականության հետևանքներն ու ապագա ուղղությունները: Համացանցի կարգավորման հետ կապված կարևոր պաշտոններում նշանակումները ոչ մի անակնկալ չմատուցեցին՝ հաստատելով Օբամայի հակումը համացանցի բացախոսության սկզբունքների հանդեպ: Նախընտրական քարոզարշավի ընթացքում տված խոստումների համաձայն, նրա թիմը ցանցային չեզոքության սկզբունքին աջակցելու մի շարք միջոցներ իրականացրեց: 2009 թ. առավել նշանակալի իրադարձությունը ԱՄՆ առևտրի նախարարության և ICANN-ի միջև «Պարտավորությունների վավերացման մասին» փաստաթղթի ստորագրումն էր, ինչը ընկերութանն ավելի անկախ պետք է դարձներ: Այդ քայլով, թեև լուծվում էր համացանցի կառավարման հիմնախնդիրներից մեկը՝ ICANN-ի գործունեության հանդեպ ԱՄՆ վերահսկողությունը, սակայն մի շարք այնպիսի այլ հարցեր էր առաջ քաշում, ինչպիսիք են՝ կազմակերպության միջազգային կարգավիճակն ու նրա գործունեության հանդեպ վերահսկողության հիմնախնդիրը: «Պարտավորությունների վավերացման մասին» փաստաթուղթը ընդգրկում է ընդհանուր ղեկավար սկզբունքներ, սակայն շատ հարցեր անպատասխան է թողնում: 2009 թ. նոյեմբերին Շարմ էշ Շեյխում (Եգիպտոս) տեղի ունեցավ IGF չորրորդ հանդիպումը: Քննարկումների բովանդակության վրա ազդել էր «Պարտավորությունների վավերացման մասին» փաստաթղթի ստորագրումը, ինչպես նաև 2010 թ. նախատեսվող երկու իրադարձություն՝ 2011 թ.-ից հետո IGF հանդիպումները շարունակելու անհրաժեշտության մասին որոշումը և Մեքսիկայում տեղի ունենալիք Հեռահաղորդակցության միջազգային միության (ՀՄՄ) հերթական համաժողովը: Չնայած որ 2009 թ. Օբամային ընտրելուց հետո բոլորի ուշադրությունը սևեռված էր ԱՄՆ-ում տեղի ունեցող իրադարձություններին, այնուամենայնիվ համացանցի կարգավորման միջազգային տեսակետները (ICANN-ի միջազգային կարգավիճակը, IGF-ի ապագան, ՀՄՄ-ի ռազմավարությունը) 2010 թ., ամենայն հավանականությամբ, առաջին պլանում կլինեն:

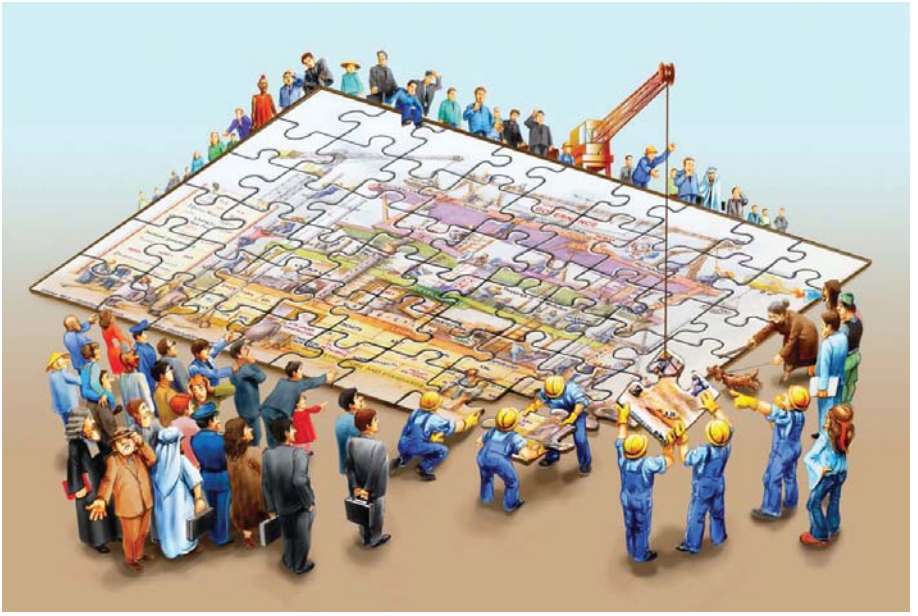
2010թ. իրադարձությունները

2010թ. օգոստոսի դրությամբ համացանցի կառավարման ոլորտի ամենաառաջնահերթ զարգացումները վերաբերել են ֆեյսբուքի, Twitter-ի և նմանատիպ սոցիալական պլատֆորմների ազդեցության աճին: Կարևորագույն խնդիրներից մեկը օգտվողների անձնական կյանքին վերաբերող գաղտնիքի պահպանումն էր: Համացանցի «աշխարհատնտեսական քաղաքականության ոլորտում» հիմնական իրադարձությունը կարելի է համարել ԱՄՆ պետքարտուղար Հիլարի Քլինթոնի ելույթը՝ համացանցում ազատ արտահայտվելու մասին, մասնավորապես, Չինաստանի եւ Google-ի խնդրի առնչությամբ: Google-ի որոնման մատչելիությունը Չինաստանում սահմանափակելու

մասին Չինաստանի իշխանությունների պահանջը հանգեցրեց այդ երկրում Google-ի որոնողական գործողությունների արգելափակմանը:
Երկու կարեւոր զարգացումներ տեղի ունեցան ICANN-ի աշխարհում. առաջին՝ արաբերեն եւ չինարեն լեզուների համար ոչ-ANSCII դոմենային անունների ներդրումը: Այլ լեզուներով դոմենային անունների խնդիրը լուծելով՝ ICANN նվազեցրել է համացանցային DNS համակարգի մասնատման վտանգը: Երկրորդ՝xxx դոմենների (մեծահասակների համար նյութերի բովանդակության) հաստատումը ICANN -ի կողմից: Այս որոշմամբ ICANN-ը հանրային քաղաքականության բարձր նշանակություն ունեցող որոշում կայացրեց համացանցի ոլորտում: Նախկինում ICANN փորձում էր գոնե ձեւականորեն մսալ տեխնիկական որոշումներ կայացնելու հարթության վրա: 2010 թ.-ին IGF-ի շարունակման մասին ՄԱԿ-ի Գիտության և զարգացման հանձնաժողովի բանաձևի ընդունմամբ սկսվեց IGF-ի վերանայման գործընթացը, որը ենթադրում է առաջիկա հինգ տարիների ընթացքում շարունակել համաժողովի աշխատանքը՝ կազմակերպչական և կառուցվածքային չնչին փոփոխություններով: 2010 թ. հուլիսին ՄԱԿ-ի Տնտեսական եւ սոցիալական հարցերով խորհուրդը (UNECOSOC) հաստատեց այդ բանաձեւը: IGF-ը շարունակելու վերաբերյալ վերջնական որոշումն ընդունվել է 2010 թ.-ի աշնանը տեղի ունեցած ՄԱԿ-ի Գլխավոր վեհաժողովի ընթացքում:

Համացանցի կառավարման վերլուծության գործիքներ

Համացանցի կառավարման վերլուծության գործիքները քաղաքական փաստարկներ նախապատրաստելու և քաղաքական ուղղություն մշակելու համար նախատեսված գործիքների հավաքածու է: Համացանցի կառավարմանը մասնակցողների համար այդ գործիքները ունեն գործնական նշանակություն: Նախ՝ այդ գործիքները կոչված են օգնելու համացանցի կառավարման հիմնախնդիրներին վերաբերող մեծածավալ տեղեկատվության, փաստաթղթերի հետ տարվող և հետազոտական աշխատանքներում կողմնորոշվելու հարցում: Երկրորդ՝ դրանք կարելի է օգտագործել քաղաքական փաստարկներ մշակելու և այլ ուղղությունների քաղաքական հայտարարությունները լավ հասկանալու համար: Վերջապես, այդ գործիքները կարող են բարձրացնել բանակցային գործընթացի արդյունավետությունը՝ բանակցող կողմերին հնարավորություն տալով բոլոր մասնակիցների համար ավելի ձեռնտու փոխզիջումներ գտնել, քան պարզապես «ընդհանուր ամենափոքր հայտարար»: Համացանցի կառավարման վերլուծական գործիքները համացանցի կառավարման ձևավորվող կարգի մի մասն են, որի կայացումը դեռ նոր է սկսվում: Միջազգային այլ կարգերի փորձը (օրինակ՝ շրջակա միջավայրի պաշտպանության, օդային տրանսպորտի կամ սպառազինության վերահսկման բնագավառներում) ցույց է տալիս, որ այդպիսի ճյուղերում



մշակվում է հայացքների, արժեքների, պատճառահետևանքային կապերի մասին պատկերացումների ընդհանուր համակարգ, փաստարկների ընդհանուր եղանակներ, տերմինաբանություն, հատուկ բառապաշար, ժարգոն, հապավումներ: Հայացքների այսպիսի համակարգը քաղաքական կյանքում մեծ նշանակություն ունի: Այն ձևավորում է տարբեր հիմնախնդիրների ըմբռնումը, ինչն իր հերթին, ազդեցություն է գործում ձեռնարկվող գործողությունների վրա: Շատ դեպքերում հայացքների համակարգի կայացման վրա ազդում է մասնագիտական առանձնահատուկ մշակույթը (միևնույն մասնագիտության ներկայացուցիչների համար մտածողության և վարքի ընդհանուր ձևերը): Ինչ-որ «ընդհանուր շրջանակների» հաստատումը օգնում է բարելավելու հաղորդակցությունը և ըմբռնումը: Սակայն երբեմն դրանք օգտագործվում են «տարածքի» պաշտպանության և արտաքին ազդեցությունը խոչընդոտելու համար: Ամերիկացի լեզվաբան Ջեֆրի Մայրելի խոսքերի համաձայն. «յուրաքանչյուր մասնագիտական լեզու ազդեցության ոլորտի լեզու է»: Համացանցի կառավարման ամեն մի գործելակարգ բարդ է լինելու, քանի որ այն պետք է ընդգրկի բազում հարցեր, մասնակիցներ, մեխանիզմներ, ընթացակարգեր և գործիքներ: Այս նկարազարդումները, որ կատարվել են հոլանդացի նկարիչ Մ. Կ. Էշերի աշխատանքների մոտիվներով, ցուցադրում են համացանցի կառավարման հետ կապված որոշ տարօրինակ տեսակետներ: Համացանցի կառավարման վերլուծական գործիքակազմն այդ ճյուղի յուրահատուկ գծերն արտացոլում է որպես «կեղտոտ» քաղաքականության հիմնախնդիրներ:[6] Համացանցի կառավարման հիմնախնդիրները, որպես կանոն, ունեն բազում կատալիզատորներ, այդ պատճառով հեշտ չէ դրանցից յուրաքանչյուրի համար երևան հանել միակ պատճառը: Շատ դեպքերում մեկ հիմնախնդիրը

մի այլ ախտանիշ է, ինչն էլ երբեմն ստեղծում է քաղաքական որոշումների «արատավոր շրջանագիծ»: Ճանաչողության որոշ մեթոդներ, ինչպիսիք են, օրինակ՝ գծային մտածողությունը, միակ պատճառի որոնումը, «կամ-կամ» մոտեցումը, միայն մասնակիորեն են կիրառելի համացանցի կառավարման հիմնախնդիրների հարցում: Համացանցի կառավարման հիմնախնդիրների վերաբերյալ միջազգային բանակցությունները ենթադրում են տարբեր հետաքրքրությունների և մոտեցումների միջև հավասարակշռության անվերջ որոնում: Համացանցի կառավարման վերլուծական գործիքակազմը ներառում է տարբեր գործիքների հավաքածու: Դրանցից մի քանիսն օգտագործվում են քաղաքական խորը հակասությունները (համացանցի կառավարման «ընդարձակ» և «նեղ» մոտեցումներ) լուծելիս, այն դեպքում, երբ մի շարք այլ գործիքներ իրենցից ներկայացնում են փաստարկների և քաղաքական խոսքի («փչացած չէ՝ մի նորոգեք») հռետորական գործելաձևեր: Եթե փորձենք կարգի բերել այդ գործիքները, ապա կարելի է առանձնացնել հետևյալ հիմնական կարգերը՝

-նմուշներ և օրինակներ,
-ղեկավար սկզբունքներ,
-համանմանություն:

Այս գործիքակազմն, ինչպես համացանցի կառավարման գործընթացը, մշտական փոփոխման է ենթարկվում: Մոտեցումները, նմուշները, ղեկավար սկզբունքները և համանմանությունները ի հայտ են գալիս ու անհայտանում տվյալ պահին բանակցությունների գործընթացի համար իրենց պատշաճության և կարևորության համաձայն:

6. «Կեղտոտ» հիմնախնդիր (wicked problem) արտահայտությունը տերմին է, որն օգտագործվում է սոցիալական գիտություններում՝ նկարագրելու համար այնպիսի հիմնախնդիր, որի լուծումը բարդ է կամ անհնար՝ կիսատ լինելու, տեղեկատվության հակասությունների, պայմանների փոփոխությունների և այլնի պատճառով: «Կեղտոտ» հիմնախնդիրները, որպես կանոն, համատեքստում այնքան են ներգրած, որ դրանց լուծումը կարող է դառնալ մի շարք նոր բարդությունների աղբյուր, բացի այդ դրանք չունեն և չեն կարող ունենալ միակ ճիշտ լուծում: Այդպիսի հիմնախնդիրները հակադրվում են պարզ, լուծելի հիմնախնդիրներին, որոնք հանդիպում են մաթեմատիկայում, շախմատում և այլն:

Մոտեցումներ և նմուշներ

Համացանցի կառավարումն ինչպես ամբողջությամբ, այնպես էլ այդ ոլորտին վերաբերող առանձին հարցեր արդեն վաղուց քաղաքական բանավեճերի և գիտական վեճերի առարկաներ են: Աստիճանաբար այդ բնագավառում ստեղծվել են մի քանի մոտեցումներ ու նմուշներ, որոնք արտացոլում

են բանակցությունների մասնակիցների դիրքորոշումների, ինչպես նաև մասնագիտական ու ազգային մշակույթների միջև տարբերությունները: Ընդհանուր նմուշների և մոտեցումների ի հայտ գալը կարող է պարզեցնել բանակցությունների գործընթացը և օգնել կառուցելու ընդհանուր «կոորդինատների համակարգ»:

«Ընդարձակ» կամ «սահմանափակ» մոտեցում

Մինչ օրս համացանցի կառավարման «սահմանափակ» և «ընդարձակ» մոտեցումների միջև դիմակայությունը համարվում է համացանցի կառավարման գործընթացում տարբեր հետաքրքրություններ արտացոլող կարևորագույն հարցերից մեկը: «Սահմանափակ» մոտեցման դեպքում ուշադրությունն, առաջին հերթին, կենտրոնացած է լինում համացանցի ենթակառուցվածքի վրա (դոմենային անունների, IP հասցեների և «արմատական» սերվերների համակարգերի) և ICANN դիրքերի վրա՝ որպես այդ դաշտի գլխավոր խաղացողի:
«Ընդարձակ» մոտեցման համաձայն, համացանցի կառավարման վերաբերյալ բանակցությունները պետք է դուրս գան ենթակառուցվածքի հարցերի սահմաններից ու դիմեն այլ՝ իրավական, տնտեսական, սոցմշակութային, զարգացման հետ կապված հարցերի: «Ընդարձակ» մոտեցումը համացանցի կառավարման հարցերով աշխատանքային խմբի հաշվետվության մեջ և տեղեկատվական հասարակության հարցերով համաշխարհային բարձր մակարդակի հանդիպման ամփոփիչ փաստաթղթերում որպես հիմք է ընդունված: Այն օգտագործվում է նաև որպես համացանցի կառավարման հարցերի վերաբերյալ ֆորումի կառուցվածքի հիմնական սկզբունք:
Այդ երկու մոտեցումների միջև տարբերությունների անցկացումը WSIS բանակցությունների ընթացքում կարևորագույն թեմա էր, սակայն այդ հարցում այդպես էլ չհաջողվեց համաձայնության հասնել: 2007 թ. նոյեմբերին Ռիո դե Ժանեյրոյում տեղի ունեցած համացանցի կառավարման հարցերով ֆորումի ընթացքում բանավեճերը ցույց տվեցին, որ «ընդարձակ» մոտեցման շրջանակներում քննարկումներն, այնուամենայնիվ, կարող են լինել միանգամայն հստակ: Ֆորումի օրակարգում համացանցի հիմնական ռեսուրսների մասին հարցի երևան գալը (այսպես կոչված՝ ICANN հիմնախնդիրը) ցույց է տալիս, որ «սահմանափակ» մոտեցման հիմնախնդիրները նույնպես պահպանում են իրենց նշանակությունը:

Քաղաքական և տեխնիկական որոշումների համաձայնեցվածություն

Համացանցի կառավարման գործում տեխնիկական և քաղաքական հարցերի ամբողջացումը հեշտ խնդիր չէ, քանի որ բարդ է դրանց միջև հստակ սահմանագիծ անցկացնելը: Տեխնիկական որոշումները չեզոք չեն: Վերջին հաշվով, յուրաքանչյուր տեխնիկական որոշում նպաստում է ինչ-որ անձանց շահերի առաջխաղացմանը, ուժեղացնում է որոշակի խմբերի դիրքերը և ազդում է հասարակական, քաղաքական ու տնտեսական կյանքի վրա: Համացանցի զարգացման վաղ փուլում դրա գործառույթների և՛

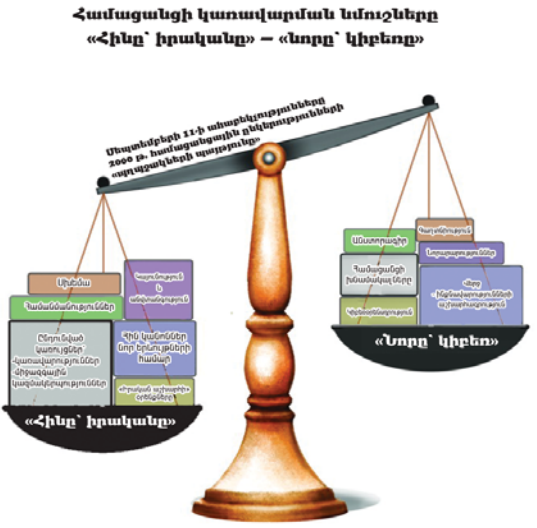
տեխնիկական, և՛ քաղաքական տեսակետները կանոնավորում էր միայն մեկ սոցիալական խումբ՝ մշակողների ու օգտվողների միությունը: Համացանցի տարածման և 1990-ականներին շահագրգիռ նոր կողմերի, առաջին հերթին՝ գործարար աշխարհի և կառավարությունների ներկայացուցիչների ի հայտ գալու հետ միասին համացանցային միությունների անդամներն արդեն չէին կարողանում «միայն ձեռքում» պահել ինչպես տեխնիկական, այնպես էլ քաղաքական հարցերի կառավարումը: Հետագա բարեփոխումները, այդ թվում՝ ICANN ստեղծումը, իրենց նպատակն էին համարում տեխնիկական և քաղաքական տեսակետների միջև հավասարակշռության վերականգնումը: Այդպիսի հավասարակշռություն գտնելու հիմնախնդիրը դեռևս լուծված չէ և մնում է համացանցի կառավարման հարցերով ֆորումի քննարկումների ընթացքում առավել վիճելի խնդիրներից մեկը:

Հին «իրական» մոտեցում կամ նոր «կիբեռմոտեցում»

Համացանցի կառավարման շրջանակում յուրաքանչյուր հարց կարելի է դիտարկել երկու տարբեր կողմերից: Հին «իրական» մոտեցման կողմնակիցները «նոր գինին հին տիկում» սկզբունքով ապացուցում են, որ համացանցը կառավարման բնագավառում ոչ մի նոր բան չի ներմուծել: Նրանց կարծիքով, կարգավորման տեսանկյունից համացանցը ևս մեկ տեխնիկական սարք է, որը չի տարբերվում իր նախորդներից՝ հեռագրից, հեռախոսից կամ ռադիոյից: Օրինակ՝ իրավական հարցերի վերաբերյալ բանավեճերի ընթացքում այս մոտեցման կողմնակիցները մատնանշում են, որ գոյություն ունեցող օրենքները մի փոքր սրբագրումից հետո կարելի է կիրառել նաև համացանցի նկատմամբ:

Տնտեսության բնագավառում այս մոտեցման համախոհները պնդում են, որ սովորական և «էլեկտրոնային» առևտրի միջև տարբերություն չկա, հետևաբար, էլեկտրոնային առևտրի իրավական հատուկ կարգավորման անհրաժեշտություն չկա:

Նոր «կիբեռմոտեցման» կողմնակիցները (այն կոչենք՝ «նոր գինին նոր տիկի մեջ») ապացուցում են, որ համացանցը հաղորդակցության, սկզբունքորեն, նոր համակարգ է՝ նախորդ բոլոր համակարգերի համեմատ: «Կիբեռմոտեցման» հիմնական առաքելությունն այն է, որ համացանցին հաջողվեց տարանջատել ժամանակակից սոցիալական և քաղաքական իրականությունը



ինքնավար պետությունների աշխարհից (աշխարհագրորեն բաժանված): Կիբեռտարածությունը իրական աշխարհից տարբերվում է, այդ իսկ պատճառով պահանջում է կառավարման այլ ձև: Իրավական ոլորտում «կիբեռմոտեցման» ներկայացուցիչները պնդում են, որ իրավասությանը, կիբեռհանցագործությանը և պայմանագրերի կնքմանը վերաբերող գոյություն ունեցող օրենքները կիրառելի չեն համացանցի նկատմամբ, այդ պատճառով էլ պետք է նոր օրենքներ ստեղծվեն:

Համացանցի կառավարման ապակենտրոնացված կամ կենտրոնացված կառուցվածքը

Ապակենտրոնացված մոտեցման համաձայն, կառավարման կառուցվածքը պետք է արտացոլի համացանցի էությունը՝ ցանցերի ցանցը: Այս մոտեցման կողմնակիցներն ընդգծում են, որ այդքան բարդ համակարգը հնարավոր չէ դնել կառավարման ընդհանուր «հովանոցի» ներքո, օրինակ՝ միջազգային կազմակերպության շրջանակներում, և որ կենտրոնացված կառավարման բացակայությունն է համացանցի արագընթաց աճի գլխավոր պատճառներից մեկը: Այս տեսակետը հիմնականում կիսում են տեխնիկական համացանցային միությունը և զարգացած երկրները:
Կենտրոնացված մոտեցման կողմնակիցները շատ բաների հետ միասին դիմում են գործնական բարդության, ինչը սահմանափակ մարդկային և ֆինանսական ռեսուրսներով երկրների համար անհրաժեշտություն է ներկայացնում մասնակցելու համացանցի կառավարման հարցերի քննարկմանը՝ ուժեղ ապակենտրոնացվածության և բազմաթիվ ինստիտուտների առկայության պայմաններում: Այդպիսի երկրների համար դժվար է դիվանագիտական հիմնական կենտրոններում (Ժնև, Նյու Յորք) մասնակցել հանդիպումների, առավել ևս հետևել այնպիսի ինստիտուտների գործունեությանը, ինչպիսիք են՝ ICANN, W3C[7] և IETF: Այդպիսի երկրները (հիմնականում՝ զարգացող) հանդես են գալիս «միասնական պատուհան» սկզբունքի կողմնակիցներ՝ նախապատվորեն որպես միջազգային կազմակերպություն:

7. W3C, World Wide Web Consortium («Համաշխարհային սարդոստայնի» կոնսորցիում) միջազգային ոչ կառավարական կազմակերպություն, որն զբաղվում է «համաշխարհային սարդոստայնի» (WWW) համար տեխնոլոգիական ստանդարտների մշակմամբ և ներդրմամբ:

Համացանցում հասարակական շահերի պաշտպանությունը

Համացանցի առավել ուժեղ կողմերից մեկը հասարակական բնույթն է, ինչն ապահովում էր ցանցի արագ աճը, ինչպես նաև խրախուսում էր կրեատիվությունն ու բաց լինելը: Համացանցի հասարակական բնույթի պաշտպանությունը կմնա համացանցի կառավարման կարևորագույն հիմնախնդիրներից մեկը: Այս հիմնախնդիրը բարդանում է այն բանով, որ համացանցի տեխնիկական ենթակառուցվածքի հիմնական մասը՝

միջմայրցամաքային գլխավոր մալուխներից մինչև տեղային ենթացանցերը, մասնավոր սեփականության մեջ են գտնվում: Կարելի՞ է, արդյոք, մասնավոր ընկերություններին պարտադրել, որպեսզի նրանք իրենց սեփականությունը ղեկավարեն՝ ծառայեցնելով հասարակական շահերին, համացանցի ո՞ր հատվածները կարելի է դիտարկել որպես հասարակական գլոբալ բարօրություն. սրանք այն բարդ հարցերից են, որոնք պարտադիր լուծում են պահանջում: Վերջին ժամանակներում համացանցի հասարակական բնույթի մասին հարցը կրկին արդիական է դարձել, ինչը պայմանավորված է ցանցային չեզոքության վերաբերյալ քննարկումներով:

Աշխարհագրությունն ու համացանցը

Համացանցի զարգացման արշալույսին տարածված էր այնպիսի մի կարծիք, ըստ որի այս գլոբալ ցանցը պետական սահմաններ է հաղթահարում և խախտում է ինքնավարության սկզբունքը: Համացանցում հաղորդակցության հանգույցները հեշտորեն հատում են ազգային սահմանները, իսկ օգտվողների անունների գաղտնիության պահպանման սկզբունքը դրված է համացանցի կառուցվածքում, ինչն էլ շատերին առիթ է տվել մեջբերում կատարելով հանրահայտ «Կիբեռտարածության անկախության հռչակագրից», ենթադրելու, որ «իշխանությունները ոչ բարոյական իրավունք ունեն ղեկավարելու մեզ (օգտվողներին), ոչ էլ պարտադրելու այնպիսի մեթոդներ ունեն, որոնք կարողանան մեզ վախեցնել»: Սակայն տեխնոլոգիաների զարգացման վերջին միտումները, այդ թվում նաև բարդ երկրալոկացիոն ծրագրային ապահովության ստեղծումը, ավելի հաճախ են հարցականի տակ դնում համացանցի դարաշրջանում «աշխարհագրության վերահաս վերջի» մասին պնդումը: Այսօր դեռևս դժվար է հստակ որոշել, թե ով է գտնվում «էկրանի մյուս կողմում», սակայն շատ հեշտ է հասկանալը, թե համացանցային ծառայություններ մատուցող ո՞ր կազմակերպության (պրովայդերի) միջոցով է տվյալ մարդը համացանց մուտք գործելու թույլտվություն ստացել: Համացանցը որքան ամուր է կապվում աշխարհագրությանն, այնքան ավելի կորցնում է իր կառավարման համակարգի առանձնահատկությունը: Օրինակ՝ օգտվողների և տարանցման գործողությունների աշխարհագրական վայրը որոշելու հնարավորության դեպքում համացանցում իրավասության բարդ խնդիրը կարող է լուծվել գոյություն ունեցող օրենքների վրա հիմնվելով:

Քաղաքական անորոշություն

Համացանցի կառավարման հարցերի վերաբերյալ բանավեճերն ընթանում են տեխնոլոգիաների զարգացման ապագա ուղղությունների վերաբերյալ անորոշության պայմաններում, իսկ այդ անորոշությունը համացանցի կառավարման բնագավառում ազդում է օրակարգի վրա: Օրինակ՝ 2002 թ., երբ նախաձեռնվեց WSIS գործընթացը, Google-ը բազմաթիվ որոնող համակարգերից մեկն էր ընդամենը: 2005 թ. նոյեմբերին՝ WSIS-ի ավարտական փուլում Google-ն արդեն համացանցի ապագան որոշող

Քաղաքական հավասարակշռության նվաճումը անցյալում

1875 թ. Միջազգային հեռագրային միությունը (ՀՄՄ-ի նախորդը) Սանկտ Պետերբուրգում համաժողով է անցկացրել, որն իր ազդեցությունն է ունեցել հեռագրի հետագա զարգացման վրա: Ամենավիճելի հարցը դարձել էր հեռագրացանցով հաղորդվող հաղորդագրությունների բովանդակության վերահսկումը: Համաժողովին մասնակցող ԱՄՆ-ն և Մեծ Բրիտանիան հանդես են գալիս որպես մասնավոր կյանքի անձեռնմխելիության և հեռագրի կիրառմամբ նամակագրության գաղտնիության պահպանման սկզբունքի կողմնակիցներ, այն դեպքում, երբ Ռուսաստանն ու Գերմանիան համառորեն պահանջում էին, որպեսզի սահմանափակվեն անձնական անձեռնմխելիությունը, որի նպատակը պետք է լիներ պետական անվտանգության, հասարակական կարգի և հասարակության բարոյականության պահպանումը: Փոխզիջման հասնել հաջողվում է դիվանագիտական հնագույն գործելաոճի՝ դիվանագիտական երկիմաստության օգնությամբ: Պետերբուրգյան համաձայնագրի 2-րդ հոդվածը երաշխավորում էր հեռագրի միջոցով իրականացվող նամակագրության գաղտնիությունը, իսկ հոդված 7-ը սահմանափակում էր մասնավոր կյանքի անձեռնմխելիությունը և թույլատրում էր պետական գրաքննության հնարավորությունը: ԱՄՆ-ն հրաժարվում է ստորագրել այդ համաձայնագիրը, գրաքննությանը հավանություն տվող հոդվածի պատճառով:

ամենաազդեցիկ ընկերություններից մեկն էր: 2002 թ. բլոգները նոր էին սկսում համբավ ձեռք բերել: Ներկայում բլոգերները կառավարություններ են քայքայում, լայնացնում են ազատ ինքնաարտահայտման սահմանները, նշանակալի ազդեցություն ունեն սոցիալական և տնտեսական կյանքի վրա: Համացանցի կառավարման հիմնախնդիրներին վերաբերող նոր տեխնոլոգիաների ցանկում ընդգրկված են Facebook, Skype, YouTube, Twitter и Wikipedia. Այսօր շատերը կարծում են, որ համացանցի կառավարման ոլորտում ի սկզբանե եղած գլխավոր հիմնախնդիրներն (ICANN գործառույթի հարցերը) աստիճանաբար կորցնում են իրենց նշանակությունը: Դրանց փոխարեն այնպիսի հարցեր են առաջ գալիս, ինչպիսիք են ցանցային չեզոքությունը, տարբեր տեխնոլոգիաների մերձեցումը (օրինակ՝ հեռախոսի, հեռուստատեսության և համացանցի), սոցիալական ցանցերի կարգավորման հիմնախնդիրները (Facebook և MySpace), ինչպես նաև Google-ի և Wikipedia-ի դերը՝ որպես թվային գիտելիքների և տեղեկատվության «պահապանների»:

Քաղաքական հավասարակշռության նվաճում

Հավանաբար, կշեռքն ամենաստույգ պատկերն է, որն արտացոլում է քաղաքականության և համացանցի կառավարման հարցերի վերաբերյալ բանավեճերի բուն էությունը: Համացանցի կառավարման շատ ճյուղեր հավասարակշռություն են պահանջում տարբեր շահերի և մոտեցումների միջև: Այդպիսի հավասարակշռությունը հաճախ փոխզիջման արդյունք է լինում: Քաղաքական «հավասարակշռությունը պահելու» մի քանի ճյուղեր գոյություն ունեն, այդ թվում՝

-ինքնարտահայտման ազատության և հասարակական կարգի պահպանման միջև հակասությունը: Համացանցում իր արտացոլումն է գտել Մարդու իրավունքների համընդհանուր հռչակագրի 19 (ինքնարտահայտման ազատություն) և 29 հոդվածների (հասարակական կարգի պահպանում)

միջև եղած հայտնի հակասությունը: Այս հակասությունը քննարկվում է համացանցում տեղ գտած նյութերի բովանդակության և գրաքննության կարգավորման համատեքստում.
-հակասություն կիբեռանվտանգության ու մասնավոր կյանքի անձեռնմխելիության միջև: Ինչպես իրական կյանքում, կիբեռտարածության մեջ անվտանգության ապահովումը վտանգի է ենթարկում մարդու որոշ իրավունքներ, այդ թվում՝ մասնավոր կյանքի անձեռնմխելիության իրավունքը: Կիբեռանվտանգության և մասնավոր կյանքի անձեռնմխելիության միջև հավասարակշռությունը մշտապես տատանվում է այս կամ այն կողմ՝ կախված աշխարհում տիրող քաղաքական իրավիճակից: 2001 թ. սեպտեմբերի 11-ի ահաբեկչությունից հետո գլոբալ օրակարգում անվտանգության հարցերն ավելի մեծ կշիռ ձեռք բերեցին և հավասարակշռությունը տեղաշարժվեց դեպի կիբեռանվտանգությունը.
- հակասություն հեղինակային իրավունքի և նյութերի բարեխղճորեն օգտագործման միջև: Սա իրական աշխարհի ևս մեկ երկընտրանք է, որն ստացել է լրացուցիչ առցանց-չափելիություն:

Քաղաքական հավասարակշռության նվաճումը անցյալում

1875 թ. Միջազգային հեռագրային միությունը (ՀՄՄ-ի նախորդը) Սանկտ Պետերբուրգում համաժողով է անցկացրել, որն իր ազդեցությունն է ունեցել հեռագրի հետագա զարգացման վրա: Ամենավիճելի հարցը դարձել էր հեռագրացանցով հաղորդվող հաղորդագրությունների բովանդակության վերահսկումը:

Մանրամասն կիբեռանվտանգության վերաբերյալ բաժին 2-ում

Համաժողովին մասնակցող ԱՄՆ-ն և Մեծ Բրիտանիան հանդես են գալիս որպես մասնավոր կյանքի անձեռնմխելիության և հեռագրի կիրառմամբ նամակագրության գաղտնիության պահպանման սկզբունքի կողմնակիցներ, այն դեպքում, երբ Ռուսաստանն ու Գերմանիան համառորեն պահանջում էին, որպեսզի սահմանափակվեն անձնական անձեռնմխելիությունը, որի նպատակը պետք է լիներ պետական անվտանգության, հասարակական կարգի և հասարակության բարոյականության պահպանումը: Փոխզիջման հասնել հաջողվում է դիվանագիտական հնագույն գործելաոճի՝ դիվանագիտական երկիմաստության օգնությամբ: Պետերբուրգյան համաձայնագրի 2-րդ հոդվածը երաշխավորում էր հեռագրի միջոցով իրականացվող նամակագրության գաղտնիությունը, իսկ հոդված 7-ը սահմանափակում էր մասնավոր կյանքի անձեռնմխելիությունը և թույլատրում էր պետական գրաքննության հնարավորությունը: ԱՄՆ-ն հրաժարվում է ստորագրել այդ համաձայնագիրը, գրաքննությանը հավանություն տվող հոդվածի պատճառով:

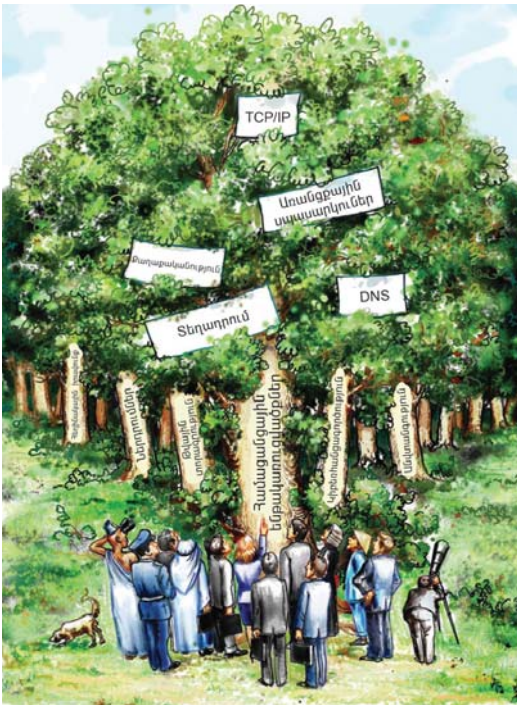
Մանրամասն մտավոր սեփականության վերաբերյալ բաժին 2-ում

Ղեկավար սկզբունքներ

Ղեկավար սկզբունքները համացանցի կառավարման կազմավորվող ռեժիմի հիմքում ընկած որոշակի արժեքներն ու հետաքրքրություններն են: Այդ սկզբունքներից մի քանիսը, ինչպիսիք են՝ մասնակցության համար թափանցիկությունն ու բաց լինելը, հավանության էին արժանացել WSIS-ում: Մյուսները ներդրվել են ոչ բացահայտորեն, համացանցի կառավարման հարցերի վերաբերյալ բանավեճերի ընթացքում:

«Անիվ մի հորինեք»

Համացանցի կառավարման ոլորտում յուրաքանչյուր նախաձեռնություն պետք է սկիզբ առնի գոյություն ունեցող նորմերի վերլուծությունից, որոնք կարելի է բաժանել երեք մեծ խմբի.
-հատուկ համացանցի համար ստեղծվածները (օրինակ՝ ICANN),
-համացանցի հետ կապված հարցերի կիրառման համար էական հարմարեցում պահանջողներ (օրինակ՝ առևտրային դրոշմանիշների պահպանումը, էլեկտրոնային առևտրի հարկադրում),
-համացանցում կիրառելիներն՝ առանց էական փոփոխությունների (օրինակ՝ խոսքի ազատության պաշտպանությունը):
Գոյություն ունեցող նորմերի կիրառումը կարող է նկատելիորեն բարձրացնել իրավական կայունությունն ու հեշտացնել համացանցի կառավարման կարգ ստեղծելու խնդիրը:



«Անսարք չէ՝ մի նորոգեք»

Համացանցի կառավարումը պետք է պահպանի համացանցի գոյություն ունեցող գործառնությունն ու հուսալիությունը, միաժամանակ պետք է բավականին ճկուն մնա՝ ի շահ տեխնիկական հնարավորությունների ընդարձակման փոփոխություններ կատարելու և լեգիտիմության բարձրացման համար: Ընդունված է այն կարծիքը, որ համացանցի կայունությունն ու գործառնությունը պետք է կառավարման հիմնական սկզբունքները լինեն: Համացանցի

կայունությունը պետք է պահպանվի՝ կիրառելով վաղուց հայտնի «աշխատող կոդ» մոտեցման ձևը, որը ենթադրում է տեխնիկական ենթակառուցվածքի մեջ աստիճանաբար ներդնել մանրակրկիտ ստուգված փոփոխությունները: Սակայն վտանգ կա, որ «Անսարք չէ՝ մի նորոգեք» կարգախոսի կիրառումը կնշանակի գոյություն ունեցող համացանցի կառավարման համակարգում որևէ փոփոխությունից անվերապահորեն հրաժարում, ներառյալ այն փոփոխությունները, որոնք պարտադիր չէ, որ կապված լինեն տեխնիկական ենթակառուցվածքի հետ: Որպես հավանական լուծումներից մեկը առաջարկվում է կիրառել այդ սկզբունքը՝ համացանցի կառավարման ոլորտում որպես կոնկրետ քայլերի գնահատման չափանիշ (օրինակ՝ որոշումներ ընդունելու մեխանիզմներում նոր արձանագրությունների և փոփոխությունների ներմուծում):

Համալիր մոտեցման և գերակայությունները որոշելու հնարավորությունը

Համալիր մոտեցումը ենթադրում է ոչ միայն տեխնիկական, այլև իրավական, սոցիալական, տնտեսական և համացանցի բարեփոխման ու գործառնական տեսակետների զարգացման հետ կապված քննարկումներ: Անհրաժեշտ է նաև հաշվի առնել թվային տեխնոլոգիաների ակտիվ մերձեցումը, ներառյալ հեռահաղորդակցության ծառայությունների փոխադրումը՝ համացանցային արձանագրությունների կիրառման համար: Կառչելով համացանցի կառավարման վերաբերյալ բանակցությունների համալիր մոտեցումից, շահագրգիռ կողմերը միաժամանակ իրենց շահերի տեսակետից պետք է որոշեն, թե որոնք են առաջնահերթ հարցերը: Ոչ զարգացող և ոչ էլ զարգացած երկրները միատարր խումբ չեն: Զարգացող երկրների միջև առաջնահերթությունների, զարգացման մակարդակի և «ՏՀՏ-պատրաստության» էական տարբերություններ կան (օրինակ՝ տեղեկատվական հաղորդակցության տեխնոլոգիաների տեսանկյունից զարգացած երկրների միջև, ինչպիսիք են՝ Հնդկաստանը, Չինաստանը, Բրազիլիան, և Սահարայից հարավ ընկած Աֆրիկայի որոշ ավելի քիչ զարգացած երկրների միջև): Համացանցի կառավարման գործում համալիր մոտեցումն ու առաջնահերթությունների սահմանումը և՛ զարգացող, և՛ զարգացած երկրների շահագրգիռ կողմերին պետք է օգնեն սևեռվելու որոշակի հարցերի շուրջ: Դա պետք է հանգեցնի առավել բովանդակալից և, հավանական է՝ պակաս քաղաքականացված բանակցությունների: Այդ դեպքում շահագրգիռ կողմերը կմիավորվեն հիմնախնդիրների շուրջ, այլ ոչ թե ավանդական քաղաքականացված «բաժանիչ ուղղությունների» (օրինակ՝ զարգացած-զարգացող երկրներ, կառավարություն-քաղաքացիական հասարակություն):

ICANN ղեկավար սկզբունքները

1998 թ. ԱՄՆ կառավարության կազմած համացանցի կառավարման վերաբերյալ «Սպիտակ գիրքը» սահմանում է ICANN ստեղծմանն առնչվող հետևյալ ղեկավար սկզբունքները.

-կայունություն. համացանցի գործառնությունը չպետք է խախտվի, հատկապես, երբ այն վերաբերում է կարևոր կառույցների աշխատանքին, ներառյալ «արմատական» սերվերները.
- մրցունակություն. կարևոր է պահպանել ստեղծագործական մոտեցումն ու ճկունությունը, ինչը կնպաստի համացանցի հետագա զարգացմանը.
-որոշումներ ընդունելը. նոր համակարգը պետք է ընդգրկի նախկինում ստեղծված համացանցի մի շարք կանոններ ու սկզբունքներ, ներառյալ կազմակերպությունը «ներքևից», բաց լինելը և այլն.
-ներկայացուցչական լինելը. նոր կառույցի մեջ պետք է մտնեն բոլոր հիմնական շահագրգիռ կողմերը ինչպես աշխարհագրական (տարբեր երկրները), այնպես էլ մասնագիտական (տարբեր մասնագիտական միությունները) իմաստով:

Տեխնոլոգիական չեզոքության սկզբունքը

Տեխնոլոգիական չեզոքության սկզբունքների համապատասխան, քաղաքական ուղղությունը մշակվում է անկախ առանձին տեխնոլոգիական կամ տեխնիկական լուծումներից: Օրինակ՝ մասնավոր կյանքի պաշտպանության ոլորտում իրավական չափանիշները պետք է սահմանեն այն, ինչը ենթակա է պաշտպանության (օրինակ՝ անձնական տվյալները, բժշկական գրառումները), այլ ոչ այն, թե ինչպես պետք է պաշտպանվի (օրինակ՝ տվյալների բազաներ մուտք գործելու թույլտվություն, տվյալների գաղտնագրում): Տեխնոլոգիական չեզոքությունը կառավարման տեսակետից բազմաթիվ առավելություններ է տրամադրում: Այն ապահովում է կարգավորող սկզբունքների երկարաժամկետ կիրառելիությունը՝ անկախ տեխնոլոգիական զարգացման հետագա ուղղություններից և հիմնական տեխնոլոգիաների հավանական համընկնումից (հեռահաղորդակցություն, ՁԼՄ, համացանց): Սակայն կարելի է նշել այս սկզբունքին հատուկ մի շարք թերություններ, հատկապես հեռահաղորդակցության բնագավառի կարգավորման գոյություն ունեցող կանոններից նորերին անցնելու դեպքերում:

Ցանցային չեզոքության սկզբունքը

Ցանցային չեզոքությունը համացանցի գլխավոր սկզբունքներից մեկն է, ինչը հնարավոր է դարձնում համացանցի վերջնական կետերի (օգտվողների և ծառայությունների) միջև տվյալների փոխանցումը, անկախ այդ տվյալների բովանդակությունից: Չեզոքության սկզբունքը հաճախ դառնում է համացանցի արագ զարգացումը պայմանավորող հիմնական պատճառ: Google, Skype и Wikipedia և այլ ընկերությունների ստեղծողները պետք է ընդամենը հետևեին մի քանի համացանցային արձանագրությունների աշխատանքին, որպեսզի կյանքի կոչեին իրենց գաղափարները: Նրանք չէին զգում թույլտվության կամ հատուկ իրավունքի կարիք, որպեսզի սեփական հայտնագործություններն օգտագործեն համացանցում բիզնես ստեղծելու համար: Ցանցային չեզոքության մասին վիճաբանությունները համացանցային ծառայությունների առևտրային նշանակալի ներուժի արդյունք են: Տարբեր

շահագրգիռ կողմեր տարբեր պատճառներով առաջարկում են մասնատել համացանց-թրաֆիկը (տեղեկատվության ծավալ): Բազմաֆունկցիոնալ մեդիաների և տեսաթրաֆիկի փոխանցման համար նոր և ավելի արագ գործող համացանցային սպասարկու ծառայությունները համացանցի առևտրային օգտագործման ամենաշահութաբեր ուղղություններից են: Այդպիսի ծառայությունների տրամադրման համար անհրաժեշտ է նոր «մակարդակ» ստեղծել, որը երբեմն կարող է նկարագրվել որպես «VIP-համացանց»: Նման որոշման հիմնական կողմնակիցներն այնպիսի խոշոր հեռահաղորդակցային ընկերություններն են, ինչպիսիք են՝ Verizon, AT&T, Comcast, զվարճանքներ արդյունաբերող և սարքավորումներ մատակարարող ներկայացուցիչները: Այդ մոտեցմանը հակադիր ցանցային չեզոքության սկզբունքը ստացել է համացանցային արդյունաբերության աջակցությունը, ներառյալ այնպիսի հսկաների, ինչպիսիք են՝ Google, eBay, Yahoo! և Amazon, օգտվողների իրավունքների պաշտպանության կազմակերպությունները, ինչպես նաև քաղաքացիական հասարակության կազմակերպությունները: Ցանցային չեզոքության սկզբունքն արդեն դարձել է բարձր քաղաքական մակարդակով քննարկումների առարկա, այդ թվում նաև ԱՄՆ Կոնգրեսում: Ցանցային չեզոքության պահպանումը ԱՄՆ նախագահ Բարաք Օբամայի տեխնոլոգիական հարցերով օրակարգի կարևորագույն սկզբունքներից մեկն է:

Ենթադրյալ տեխնիկական որոշումները վերածեք պարզ քաղաքական սկզբունքների

Համացանցային միությունում տարածում է գտել այն կարծիքը, որ համացանցի տեխնիկական սարքավորումների առանձնահատկությունները նպաստում են հասարակական որոշակի արժեքների տարածմանը, օրինակ՝ շփման ազատությանը: Օրինակ՝ ցանցային չեզոքության սկզբունքը, որի համաձայն ցանցում երկու վերջնակետերի միջև տվյալները փոխանցվում են առանց «միջնորդների» ներգրավման, հաճախ հռչակվում է համացանցում խոսքի ազատության երաշխավոր: Դրանից կարելի է սխալ հետևություն անել, որ տեխնոլոգիական որոշումներն ինքնին բավական են հասարակական արժեքների պահպանման և առաջխաղացման համար: Վերջին ժամանակներում համացանցի զարգացումը ապացուցում է (օրինակ՝ «միջցանցային պաշտպանական էկրանի-Brandmauer»-ի կիրառումը՝ տեղեկատվության հոսքը սահմանափակելու համար), որ տեխնոլոգիան կարելի է օգտագործել տարբեր, այդ թվում՝ փոխադարձորեն միմյանց հակասող նպատակներով: Երբ դա հնարավոր է, քաղաքական սկզբունքները, ինչպիսին է՝ հաղորդակցության ազատությունը, պետք է հստակորեն նշված լինեն քաղաքական մակարդակով, այլ ոչ թե անորոշ ենթադրություն արվի տեխնիկական մակարդակով: Տեխնիկական լուծումները կոչված են նպաստելու քաղաքական սկզբունքների իրականացմանը, սակայն չպետք է լինեն դրանց առաջխաղացման միակ միջոցը:

Հիշեք ծրագրային կոդի օգնությամբ հասարակությանը կառավարելու ռիսկերի մասին

Լորենս Լեսինգը «Կոդը և կիբեռտարածության այլ օրենքները» գրքում ուշադրության է արժանացնում տեխնոլոգիայի և քաղաքականության միջև փոխհարաբերությունների հիմնական տեսակետներից մեկը, այն, որ համացանցից կախվածության աստիճանի համապատասխան, ժամանակակից հասարակությունը սկսում է կարգի հրավիրվել ոչ թե օրենքներով, այլ ծրագրային կոդերով: Վերջին հաշվով, կառավարությունների և խորհրդարանների մի շարք օրենսդրական գործառույթներ դե ֆակտո կարող են ստանձնել համակարգչային ընկերություններն ու ծրագրեր մշակողները: Ծրագրերով ապահովման և տեխնիկական լուծումների օգնությամբ նրանք կարող են ազդեցություն գործել համացանցից ավելի ու ավելի կախվածություն ունեցող հասարակության կյանքի վրա: Եթե հասարակությունը ղեկավարվի կոդի (այլ ոչ օրենքների) օգնությամբ, դա իրական մարտահրավեր կլինի արդի հասարակության կյանքի քաղաքական և իրավական կազմակերպման հիմունքներին:

Համանմանություններ

Թեև համանմանությունները հաճախ խաբուսիկ են,
սակայն ավելի պակաս խաբուսիկ, քան որևէ այլ բան:
Անգլիացի գրող Սամուել Բաթլեր (1835–1902)

Համանմանությունները մեզ օգնում են հասկանալու նոր երևույթներն արդեն հայտնիների միջոցով: Անցյալում և ներկայում կատարվող օրինակների միջև զուգահեռների անցկացումը, չնայած դրա հետ կապված վտանգին, քաղաքականության և իրավունքի մեջ հիմնական ճանաչողական գործընթաց է: Համացանցի հետ կապված դատական գործերի մեծ մասը լուծվում է համանմանությունների միջոցով: Համացանցի կառավարման գործում համանմանությունների կիրառումը մի շարք կարևորագույն սահմանափակումներ ունի: Առաջին՝ համացանցը լայն հասկացություն է, որն ընդգրկում է բազմազան ծառայություններ՝ էլեկտրոնային փոստ (տես՝ համանմանություն հեռախոսի հետ), WWW «համաշխարհային սարդոստայնի» ծառայությունները (տես՝ հեռա և ռադիոհաղորդումների հետ համանմանությունները) և տվյալների բազաները (տես՝ գրադարանի հետ համանմանությունները):

Համացանցի որևէ տեսակետի հետ յուրաքանչյուր համանմանություն կարող է չափից ավելի պարզեցնել տվյալ տեխնոլոգիայի ըմբռնումը:

Երկրորդ՝ տարբեր հեռահաղորդակցությունների և մեդիա-ծառայությունների մերձեցման համապատասխան, դրանց միջև եղած ավանդական տարբերությունները վերանում են: Օրինակ՝ համացանցային հեռախոսության (VoIP) տեխնոլոգիան ներմուծելով, ավելի դժվարանում

է սահմանազատում մտցնել համացանցի և հեռախոսակապի միջև: Սակայն, չնայած այդ սահմանափակումներին, դատական գործերի լուծման և համացանցի կառավարման կարգն ստեղծելու ընթացքում համանմանությունները մտում են հիմնական ճանաչողական գործիքները: Ավելի հաճախ կիրառվող համանմանություններից մի քանիսը քննարկվում են ստորև:

Համացանց - հեռախոսակապ

Ընդհանուր գծեր

Համացանցի զարգացման վաղ շրջանում այդ համանմանության ի հայտ գալուն նպաստեց այն փաստը, որ հեռախոսագծերն օգտագործվում էին համացանց կոմուտատորական հասանելիության համար: Դրա հետ միասին, հեռախոսի ու համացանցի միջև (էլեկտրոնային փոստի և չաթի) գոյություն ունի նաև գործառնական նմանություն՝ երկուսն էլ անմիջական ու անձնական շփման միջոց են:

Հեռախոսի և համացանցի միջև ավելի ուշ շրջանի համանմանությունը ուշադրություն է դարձնում հեռախոսային համարների համակարգի հավանական օգտագործմանը՝ դոմենային անունների համակարգն ստեղծելիս:

Տարբերությունները

Համացանցում տվյալների փոխանցման հիմքում տվյալների փաթեթի կիրառումն է, այլ ոչ թե էլեկտրական շղթաների (ինչպիսին հեռախոսային կապի դեպքում է): Ի տարբերություն հեռախոսային կապի, համացանցում չի կարելի երաշխավորել ծառայությունների տրամադրում, այլ ընդամենը կարելի է խոստանալ, որ դրա համար «բոլոր ջանքերը» կգործադրվեն: Այդ համանմանությունն արտացոլում է հաղորդակցության միայն մեկ տեսանկյուն՝ էլեկտրոնային փոստի կամ չաթի կիրառումը: Համացանցի օգտագործման այլ կարևոր միջոցները՝ «համաշխարհային սարդոստայնը» (WWW), մուլտիմեդիան և այլն, հեռախոսի հետ նմանություն չունեն:

Ո՞վ է կիրառում

Համացանցի նյութերի յուրաքանչյուր էական կարգավորման հակառակորդները (հիմնականում՝ ԱՄՆ-ում): Եթե համացանցը նման է հեռախոսին, ապա համացանցով փոխանցվող տվյալներն, ինչպես հեռախոսային խոսակցությունները, չպետք է վերահսկվեն: Այս

Փոստային համակարգը և ICANN-ը

ICANN-ի տնօրենների խորհրդի նախկին ղեկավար Փոլ Թումին փոստային համակարգի և ICANN գործառույթների միջև հետևյալ համանմանությունն է արել. «Համացանցը եթե ներկայացնենք որպես փոստային համակարգ, ապա դոմենային անուններն ու IP հասցեներն, ըստ էության, երաշխավորում են, որ նամակը տեղ կհասնի ծրարի վրա գրված հասցեով: Նրանք գործ չունեն այն բանի հետ, թե ինչ կա ծրարում, ով է ծրարն ուղարկում, ով իրավունք ունի նամակը կարդալու, որքան ժամանակում ծրարը կհասնի հասցեատիրոջը, ինչ արժի այն ուղարկելը: Այս հարցերից ոչ մեկը ICANN-ի համար կարևոր չէ: Դրա գործառույթը միայն երշխավորելն է, որ նամակը կհասնի հասցեատիրոջը»:

համանմանությունը կիրառում են նաև նրանք, ովքեր ապացուցում են, որ հաղորդակցման մյուս համակարգերի նման (օրինակ՝ հեռախոսային կապը, փոստը) համացանցը ևս պետք է վերահսկեն իշխանության ազգային մարմինները՝ միջազգային կազմակերպությունների համակարգող դերի ներքո, ինչպիսին է Հեռահաղորդակցության միջազգային միությունը:[6]

Համացանց-փոստ

Ընդհանուր գծեր

Համանմանություններ գոյություն ունեն գործառույթների, հատկապես հաղորդագրությունները հասցեատերերին հասցնելու առումով: «Էլեկտրոնային փոստ» անվանումն ինքնին ընդգծում է այդ համանմանությունը:

Տարբերությունները

Այս համանմանությունը վերաբերում է համացանցային սպասարկումներից միայն մեկին՝ էլեկտրոնային փոստին: Բացի այդ, փոստն ուղարկողի և ստացողի միջև փոստային ծառայությունն ավելի բարդ միջնորդական կառույց է, քան էլեկտրոնային փոստի համակարգը, որում միջնորդի դերը կատարում է համացանցային ծառայություններ մատակարարողը կամ Yahoo!-ի կամ Hotmail-ի նման փոստային համակարգը:

Ո՞վ է կիրառում

Համաշխարհային փոստային պայմանագիրն այս համանմանությունն անցկացնում է սովորական և էլեկտրոնային փոստի միջև՝ վերջինս սահմանելով որպես «փոստային ծառայություն, որը հեռահաղորդակցություններն օգտագործում է հաղորդագրություններ փոխանցելու համար»: Այս համանմանությունը կարող է կարևոր հետևանքներ ունենալ, օրինակ՝ պաշտոնական փաստաթղթերը տեղ հասցնելու առումով: Այսպես, օրինակ՝ էլեկտրոնային փոստով դատարանի որոշումն ստանալն այդ դեպքում պետք է համարվի համապատասխան փաստաթղթի պաշտոնապես հանձնում:

Իրաքում զոհված ամերիկյան զինվորների ընտանիքները փորձում էին բողոքարկել մասնավոր նամակագրության (նամակների) և էլեկտրոնային փոստի միջև համանմանությունների դեմ, որպեսզի թույլտվություն ստանային ձեռք բերելու իրենց հարազատների էլեկտրոնային հաղորդագրություններն ու բլոգները (առցանց-օրագրեր) ՝ ապացուցելով, որ իրենք պետք է ժառանգեն էլեկտրոնային նամակներն ու բլոգները, ինչպես ժառանգվում են սովորական նամակներն ու օրագրերը:

Համացանցային ծառայություններ մատակարարողների համար այնքան էլ հեշտ չէր փոթորկուն զգացմունքներ առաջացնող այդ հիմսախնդիրը լուծել: Համացանցային ծառայություններ մատակարարողների մեծ մասը նամակների և էլեկտրոնային փոստի միջև համանմանությունն ընդունելու փոխարեն, մերժում է թույլտվությունը՝ վկայակոչելով օգտվողների հետ կնքած պայմանագիրը՝ նամակագրության գաղտնիությունը պահպանելու մասին:

Համացանց - հեռուստատեսություն

Ընդհանուր գծեր

Ի սկզբանե համանմանությունը կապված էր հեռուստացույցի և համակարգչի էկրանների արտաքին նմանության հետ: Մեծ լսարանին հաղորդումներ տալու համար ավելի նրբին համանմանությունը հաղորդակցության երկու միջոցներն էլ՝ համացանցն ու հեռուստացույցը օգտագործում է:

Տարբերությունները

Համացանցը տվյալներ հաղորդելու ավելի մեծ հնարավորություններ ունի, քան հեռուստացույցը: Թեև հեռուստացույցի և համակարգչի էկրանի նմանությունն ակնհայտ է, սակայն դրանց միջև գոյություն ունեն կարևոր կառուցվածքային տարբերություններ: Հեռուստացույցը հնարավորություն է տալիս տեղեկատվությունը հաղորդել «մեկից՝ շատերին», իսկ համացանցը հնարավոր է դարձնում հաղորդակցության տարբեր ձևերը՝ «միմյանց հետ», «մեկը՝ շատերի հետ», «շատերը՝ շատերի հետ»:

Ո՞վ է կիրառում

Այս համանմանությունն օգտագործում են նրանք, ովքեր ձգտում են ավելի խստորեն վերահսկել համացանցի նյութերի բովանդակությունը: Նրանց կարծիքով, քանի որ համացանցի՝ որպես զանգվածային լրատվամիջոցի հնարավորությունները նման են հեռուստատեսության հնարավորություններին, ապա համացանցը պետք է խստորեն վերահսկել: ԱՄՆ կառավարությունը փորձում էր օգտագործել այդ համանմանությունը «Ռինոն ընդդեմ Հանուն քաղաքացիական ազատության ամերիկյան միության» (Reno vs. ACLU) հանրահայտ գործում: Այդ գործի սկզբնաղբյուրը դարձավ հաղորդակցության պատշաճության մասին Կոնգրեսի ընդունած փաստաթուղթը, որը նախատեսում էր համացանցի նյութերի բովանդակության մանրազնին վերահսկողություն, որպեսզի կանխվի պոռնոգրաֆական նյութեր դիտելու երեխաների իրավունքը : Դատարանը հրաժարվեց ճանաչել հեռուստատեսության հետ համանմանության լիիրավությունը:

Համացանց-գրադարան

Ընդհանուր գծեր

Համացանցը երբեմն դիտարկում են որպես տեղեկատվության հսկա պահոց և այն նկարագրելու համար կիրառում են «գրադարան», «թվային վիթխարի գրադարան», «կիբեռգրադարան», «21-րդ դարի Ալեքսանդրյան գրադարան» և այլ նմանատիպ տերմիններ:

ICANN-ի տնօրենների խորհրդի նախկին ղեկավար Պոլ Թումին փոստային համակարգի և ICANN գործառույթների միջև հետևյալ համանմանությունն է արել. «Համացանցը եթե ներկայացնենք որպես փոստային համակարգ, ապա դոմենային անուններն ու IP հասցեներն, ըստ էության, երաշխավորում են, որ նամակը տեղ կհասնի ծրարի վրա գրված հասցեով: Նրանք գործ չունեն այն բանի հետ, թե ինչ կա ծրարում, ով է ծրարն ուղարկում, ով իրավունք ունի նամակը կարդալու, որքան ժամանակում ծրարը կհասնի

հասցեատիրոջը, ինչ արժի այն ուղարկելը: Այս հարցերից ոչ մեկը ICANN-ի համար կարևոր չէ: Դրա գործառույթը միայն երշխավորելն է, որ նամակը կհասնի հասցեատիրոջը»:

Տարբերությունները

Տեղեկատվության և տվյալների պահպանումը համացանցի տեսանկյուններից ընդամենը մեկն է: Համացանցի և գրադարանի միջև կարևոր տարբերություններ կան: Դրանք են՝

-ավանդական գրադարանները, սովորաբար, սպասարկում են որոշակի տեղանքում բնակվող մարդկանց (քաղաքում, երկրում և այլն), իսկ համացանցը համաշխարհային երևույթ է.

-գրքերն ու հոդվածները սովորաբար հրատարակվում են որակը վերահսկող երաշխիքների (խմբագրական աշխատանք) որոշակի ընթացակարգ պահպանելով: Համացանցում տեղադրված նյութերը միշտ չէ, որ խմբագրվում են.

-գրադարանի նյութերը դասավորվում են դրանց որոնումը հեշտացնող որոշակի կարգով: Իսկ համացանցում դասակարգման այդպիսի սխեմա չկա, բացի մի քանի կատալոգներից (ինչպիսին Yahoo! է), որոնք թվայնացնում են հասանելի տեղեկատվության միայն մի որոշ մասը.

- բացի մատենագիտական նկարագրությունից, գրադարանում պահպանվող նյութերը (գրքերի և հոդվածների տեքստեր) ընթերցողին անհասանելի են այնքան ժամանակ, քանի դեռ նա որևէ գիրք չի վերցնում: Համացանցում տեղեկատվությունը բաց է բոլորի համար, և յուրաքանչյուրն այն կարող է անմիջապես ստանալ որոնող համակարգերի շնորհիվ:

Ովքեր են կիրառում

Կիրառում են մասնագետները տարբեր նախագծերում, որոնց նպատակն է ստեղծել որոշակի հարցերի (տվյալների բազա, պորտալներ և այլն) վերաբերյալ տեղեկատվության և գիտելիքների համապարփակ համակարգ: Վերջին ժամանակներում գրադարանի հետ համանմանությունը օգտագործվում է Google Books-ի նախագծի ծրագրերում, որի հիմնական խնդիրը տպագիր բոլոր հրատարակությունների թվայնացումն է:

Համացանց- տեսամագնիտոֆոն, պատճենահանման սարք

Ընդհանուր գծեր

Այս համանմանության հիմնական կողմը նյութերի վերարտադրումն ու տարածումն է (օրինակ՝ գրքերի տեքստեր): Համակարգիչները կրկնօրինակների ստեղծման գործը պարզեցրել են ի հաշիվ «պատճենելու և տեղադրելու» գործառույթի: Դա էլ, իր հերթին, պարզեցրել է տեղեկատվության տարածումը՝ համացանցն օգտագործելով:

Տարբերություններ

Համակարգչի գործառույթները չեն սահմանափակվում նյութերի կրկնօրինակմամբ, թեև համացանցում կրկնօրինակման գործընթացն ավելի պարզ է, քան տեսամագնիտոֆոնով կամ պատճենահանման սարքով:

Ով է կիրառում

Այս համանմանությունն օգտագործվում էր ԱՄՆ-ում ընդունված Թվային դարաշրջանում հեղինակային իրավունքի (Digital Millennium Copyright Act, DMCA) մասին օրենքի կապակցությամբ, որը պատասխանատվություն էր սահմանում այն կազմակերպությունների (օրինակ՝ համապատասխան ծրագրային ապահովում մշակող) համար, որոնք նպաստում են հեղինակային իրավունքի խախտմանը: Այսպիսի դեպքերում հակափաստարկ է այն, որ ծրագրային ապահովում մշակողները, ինչպես նաև տեսամագնիտոֆոններ ու պատճենահանման սարքեր արտադրողներն, անկասկած, չեն կարող իմանալ, թե արդյոք կարճ է իրենց արտադրանքը անօրինական նպատակներով օգտագործվել: Այս համանմանությունն օգտագործվել է պիրինգի (անմիջականորեն օգտվողների համակարգիչների միջև) սկզբունքով ֆայլերի փոխանակման համար, ինչպիսիք են՝ Grokster-ը և StreamCast-ը, ծրագրային ապահովում մշակողների դեմ հարուցված դատական գործերում:

Համացանց-մայրուղի

Ընդհանուր գծեր

Այս համանմանությունը կախված է այն բանից, թե նոր բացահայտումներն ու նոր նվաճումները որքանով կիմայեն ամերիկացիներին: Երկաթուղիները և մայրուղիները, որպես կանոն, այդ գործընթացի մի մասն են կազմում: Համացանցը որպես գործուն աշխարհի սահման, փոխաբերաբար հարաբերակցվում է իրական աշխարհի մայրուղիների հետ:

Տարբերությունները

Տեղեկատվության «փոխադրելու-հաղորդելու» հայեցակարգից բացի, համացանցի և մայրուղու միջև այլ նմանություն չկա:Համացանցով փոխադրվում-հաղորդվում են աննշմար նյութեր (տվյալներ), իսկ ճանապարհները թեթևացնում են մարդկանց և ապրանքների տեղաշարժի բեռնվածությունը:

Ով է կիրառում

Ավտոմայրուղու հետ համանմանությունը 1990-ականների կեսերից ակտիվորեն սկսեց կիրառվել այն բանից հետո, երբ Ա. Գորը գործածության

Համացանցն ու մայրուղիները

ՀՄՄ գլխավոր քարտուղար Համադուն Տուրեն ավտոմայրուղու հետ համանմանությունն օգտագործում էր ավտոմայրուղիները հեռահաղորդակցության ցանցերի, իսկ համացանց-թրաֆիկը՝ բեռնատարների կամ ընդհանրապես մեքենաների հետ համեմատելով. «Ես մի պարզ օրինակ բերեցի՝ համացանցը և տվյալների փոխանցումը համեմատելով ավտոմայրուղու բեռնատարների կամ ավտոմեքենաների հետ: Այն, որ դուք ավտոմայրուղու սեփականատերն եք, իրավունք չի տալիս ձեր սեփականությունը համարել այդ մայրուղով անցնող մեքենաներն ու բեռնատարները և, իհարկե, այն ապրանքը, որ նրանք փոխադրում են: Սա պարզ համանմանություն է: Սակայն, որպեսզի տրանսպորտն անխափան երթևեկի, ճանապարհների և կամուրջների շինարարության ժամանակ պետք է հաշվի առնել բեռնատարների քաշը, բարձրությունն ու արագությունը: Հակառակ դեպքում համակարգը չի աշխատի: Իմ կարծիքով, սա արտացոլում է համացանցի և հեռահաղորդակցության ցանցերի միջև փոխադարձ կապը: Դրանք դատապարտված են համատեղ աշխատելու»:[7]

մեջ մտցրեց «տեղեկատվական գերմայրուղի» (information superhighway) տերմինը: «Մայրուղի» տերմինը կիրառեց նաև Գերմանիայի կառավարությունը, որպեսզի արդարացներ 1997 թ. հունիսին համացանցի բովանդակությունը վերահսկելու մասին առավել խիստ օրենքի ընդունումը. *«Դա ազատական օրենք է, որը գրաքննության հետ ոչ մի ընդհանուր բան չունի, սակայն հստակորեն նշում է, թե ինչ կարող է և չի կարող անել պրովայդերը: Համացանցը գիտելիքներ հաղորդելու և տարածելու միջոց է, ինչպես մայրուղիների համար անհրաժեշտ են երթևեկության կանոնները»:*

Համացանց-բաց ծով

Ընդհանուր գծեր

Այս համանմանությունն ի սկզբանե ծագել է այն բանի շնորհիվ, որ համացանցը բաց ծովի պես պետությունների իրավասության սահմաններից դուրս էր: Այսօր ակնհայտ է, որ համացանցի մեծ մասն այս կամ այն երկրի իրավասության ներքո է: Տեխնիկական ենթակառուցվածքը, որի միջոցով փոխանցվում է համացանցային թրաֆիկը, որպես կանոն, հեռահաղորդակցության օպերատոր ընկերությունների մասնավոր և պետական սեփականությունն են: Այս իմաստով ամենամերձ համանմանությունը բեռնարկղեր փոխադրող նավարկելի ընկերություններն են:

Տարբերությունները

Ծովային տրանսպորտը կարգավորվում է միջազգային լայնածավալ համաձայնագրերով, որը սկիզբ է առնում ծովային իրավունքի վերաբերյալ պայմանագրերից: Դրա դրույթները զարգացնում և լրացնում են շրջակա միջավայրի պաշտպանության կամ անվտանգության ապահովման հիմնախնդիրները կարգավորող ծովային միջազգային կազմակերպությունների ընդունած բազմաթիվ պայմանագրերը: Այդ պայմանագրերը կարգավորում են պետական իրավասության սահմաններից դուրս, օրինակ՝ բաց ծովում իրականացվող գործունեություն: Համացանցում տվյալների փոխանցման առումով նման բան գոյություն չունի:

Ո՞վ է կիրառում

Այս համանմանությունն օգտագործում են համացանցի միջազգային կարգավորման կողմնակիցները: Դրա հետևանքը գործնականում այն է, որ համացանցի համար կիրառելի է հռոմեական իրավունքի՝ res communis omnium (համընդհանուրի ժառանգություն) հայեցակարգը, ինչը կիրառվում է բաց ծովի հանդեպ:

Համացանցի կառավարման հարցերի դասակարգումը

Համացանցի կառավարումը նոր ու բարդ բնագավառ է, որ պահանջում է «քարտեզի վրա նախնական նշում» և դասակարգում: Համացանցի կառավարման բարդությունը կապված է նրա միջկարգապահական բնույթի հետ, որն ընդգրկում է տեխնոլոգիա, հասարակական տնտեսական

հարցեր, զարգացում, իրավունք և քաղաքականություն: Դասակարգման գործնական պահանջը ցայտունորեն արտահայտվել է WSIS գործընթացում: Սկզբնական փուլում, 2003 թ. Ժնևի հանդիպմանը նախապատրաստվելու ընթացքում, մասնակիցներից շատերը այնքան էլ հեշտ չէին գլուխ հանում համացանցի կառավարման բոլոր նրբություններից: Տարբեր հետազոտական աշխատություններում, ինչպես նաև համացանցի կառավարման հարցերով աշխատանքային խմբի (WGIG) ամփոփիչ հաշվետվության մեջ առաջարկվող բարդ դաշտի կոնցեպտուալ սխեման նպաստել է բանակցային WSIS գործընթացի արդյունավետության բարձրացմանը: WGIG-ի (2004 թ.) ամփոփիչ հաշվետվության մեջ նշվում են հետևյալ կարևորագույն հիմնախնդիրները.

-կարևորագույն համացանցային ռեսուրսների կառավարմանն ու ենթակառուցվածքին վերաբերող հարցեր,

-համացանցի օգտագործմանը վերաբերող հարցեր, ներառյալ սպամը, ցանցային անվտանգությունն ու կիբեռհանցագործությունը,

-համացանցի հետ կապված, սակայն հեռուն գնացող հետևանքներ ունեցող հարցեր, որոնք դուրս են համացանցի շրջանակներից և որոնց համար պատասխանատու են համապատասխան գործող կազմակերպությունները, օրինակ՝ մտավոր սեփականության իրավունքի կամ միջազգային առևտրի հարցերը,

-համացանցի կառավարման համատեքստում զարգացման հիմնախնդիրներին, մասնավորապես՝ զարգացող երկրների ներուժի ամրապնդմանը վերաբերող հարցեր:

2006 թ. Աթենքում տեղի ունեցած Համացանցի կառավարման առաջին համաժողովի օրակարգում ընդգրկված էր հետևյալ լուծում պահանջող ոլորտների քննարկումը՝

- համացանցի մատչելիություն,
- անվտանգություն,
- համացանցի բաց բնույթ և անխոչընդոտ գործածում,
- բազմազանություն:

Երկրորդ IGF-ի ընթացքում, որը տեղի ունեցավ 2007 թ. Ռիո դե Ժանեյրոյում, օրակարգ մտցվեց հինգերորդ լուծում պահանջող ոլորտը՝

- համացանցի կարևորագույն ռեսուրսների միջոցով կառավարումը:

Դասակարգման հանդեպ մոտեցումների տարբերություններով հանդերձ,

համացանցի կառավարումը շոշափում է համեմատաբար հաստատուն 40-50 կոնկրետ հիմնախնդիրներ: Դրանցից յուրաքանչյուրի հրատապությունը կարող է փոխվել: Մասնավորապես, 2004 թ. WGIG դասակարգման մեջ որպես առանձին հիմնախնդիր էր դիտարկվում սպամը, սակայն IGF հանդիպման ընթացքում դրա քաղաքական նշանակությունը նվազում է, և սպամն ընդամենը դառնում է անվտանգության հիմնախնդիրների շրջանակում քննարկվող ոչ էական թեմաներից մեկը: Համացանցի կառավարման տեսակետների մշակված Diplo դասակարգումը համացանցի կառավարման հիմնական խնդիրները բաժանում է հինգ խմբի: Տերմինաբանությունը դիվանագիտության աշխարհին մոտեցնելու համար Diplo-ն կիրառում է «զամբյուղ» հասկացությունը (դիվանագիտական գործառնություններում այն մտցվել է Եվրոպայում անվտանգության և համագործակցության հարցերով խորհրդակցության (ԵԽԱՀ) ժամանակ): 1997 թ.-ից, երբ Diplo հիմնադրամը սկսում է դասակարգչի մշակումը, կիրառվում է հինգ զամբյուղ.

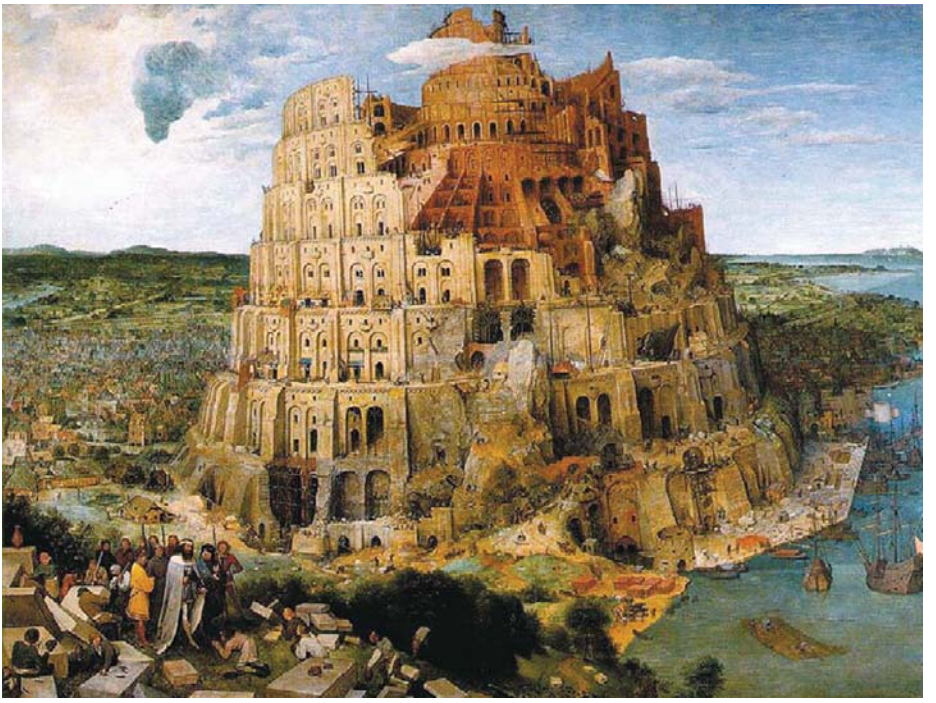
1. ենթակառուցվածք և միջոցների ստանդարտացում,
2. իրավական տեսակետներ,
3. տնտեսական տեսակետներ,
4. զարգացման հետ կապված տեսանկյուններ,
5. սոցմշակութային տեսակետներ:

Diplo-ի մշակած դասակարգումն արտացոլում է, ինչպես վերը հիշատակված WGIG և IGF քաղաքական մոտեցումները, այնպես էլ տվյալ ոլորտում գիտական հետազոտությունների արդյունքները: Դասակարգումն անդադար ճշտվում և լրացվում է՝ հաշվի առնելով Diplo-ի կրթական ծրագրերի մասնակիցների մեկնաբանությունները (2009 թ. 700 շրջանավարտ), գիտական ուսումնասիրությունների և քաղաքական փորձի արդյունքները: «Հինգ զամբյուղի» նմուշը փոխաբերաբար ներկայացված է Diplo-ի ուսումնասիրողների մշակած «Կառուցվող շենք» պատկերում:

«Կառուցվող շենք». Համացանցի կառավարում՝ արդյոք չքնաք կառուցում 21-րդ դարի բաբելոնյան աշտարակը

Վիեննայի արվեստի պատմության թանգարանում գտնվող Պիտեր Բրեյգել Ավագի (1563) նկարը պատկերում է Բաբելոնի աշտարակի կառուցումը (իսկ չափսերով ավելի փոքր մեկ այլ նկար նույն թվականին և նույն սյուժեով նկարված, ցուցադրված է Ռոտերդամի Բոյմանս վան Բեյնինհենի թանգարանում): Աստվածաշնչում ասվում է (Մատ. 11.7), որ Աստված թույլ չտվեց մարդկանց ավարտել աշտարակի կառուցումը՝ խառնելով շինարարների լեզուները «այնպես, որպեսզի նրանք միմյանց չհասկանան»: Համացանցի վերաբերյալ հարցերը քննարկելիս Բաբելոնի աշտարակի կառուցման հետ համանմանությունը միանգամայն տեղին է: Այդ համեմատությունը հեղինակներին մղեց դեպի մեկ այլ կառուցվող


SOCKETS
XSLT
HTML
XML
CSS
SMTP
TCP/IP
DNS
IP v4
FTP
END-TO-END NETWORKS
INTEROPERABILITY
PACKET SWITCHING
SSL
RFC
IM
IRC
X.25



շինություն, որի նպատակը ոչ թե երկնքին հասնելն է, այլ երկրագնդում ապրող յուրաքանչյուր մարդուն դիպչելն է: Համացանցի կառավարման վերաբերյալ քննարկումների համար Diplo-ի աշխատակիցները մշակեցին ընդհանուր նախագիծ, ինչը պատկերված է նախորդ էջի նկարում: Շենքի յուրաքանչյուր հարկ քննարկվում է հաջորդ գլուխներում: Կարևոր է հասկանալ, որ շենքի բոլոր հարկերը իրար հետ կապված են, իսկ շենքի շինարարությունը միշտ շարունակվում է և երբեք չի ավարտվի:

Ծանոթագրություն.

1.Համացանցի աճը բնութագրող ցուցանիշները հարկ է ընկալել մի քիչ թերահավատորեն և զգուշորեն: Ներկայում շատ փաստեր հաստատում են, որ 1990-ականների վերջին սկսված հեռահաղորդակցության իրարանցումը և այդ հատվածում խոշոր ներդրումների տապալումը արդյունք էին միանգամայն ոչ իրատեսական գնահատականների, որոնց համաձայն, համացանց-թրաֆիկը պետք է կրկնապատկվեր յուրաքանչյուր երեք ամիսը մեկ: Այս՝ արմատապես սխալ ենթադրությունը, մի շարք դեպքերում հիշատակել են նաև հեռահաղորդակցության ոլորտում աշխատող պետական չինովնիկները, այդ թվում՝ ԱՄՆ կապի դաշնային հանձնաժողովի ղեկավար Ռիդ Հանտը:

Այս ֆենոմենը նկարագրված է մի շարք հոդվածներում, այդ թվում՝ Andrew Odlyzko, “Internet Growth: Myth and Reality, Use and Abuse” 8 (համացանցի հասցեն՝ http://www.dtc.umn.edu/~odlyzko/doc/internet.growth.myth.pdf), ինչպես նաև “Internet as Hyperbole” (համացանցի հասցեն՝ http://folk.uio.no/gisle/essay/diff .html):

2. Այս սահմանումը հիմնվում է միջազգային կարգերի տեսության դրույթների վրա: Միջազգային կարգերի տեսության հիմնադիր Սթիվեն Կրասները նշում է, որ *«կարգը կարող է սահմանվել որպես բացահայտ և ոչ բացահայտ սկզբունքների, նորմերի, կանոնների և որոշումներ ընդունելու ընթացակարգերի հավաքածու, որոնց շուրջ միջազգային հարաբերությունների այս ճյուղի հեղինակների սպասումները համընկնում են: Սկզբունքները փաստերի, պատճառահետևանքային կապերի և բարոյականության չափանիշների մասին պատկերացումներն են: Չափանիշները պարտականությունների և իրավունքների մասին տերմիններում սահմանված վարքի ստանդարտներն են: Կանոնները յուրահատուկ արգելքներ են և գործողության կարգադրություն: Որոշումներ կայացնելու ընթացակարգերը համախմբված (կոլեկտիվ) որոշումներ ընդունելու և իրականացնելու գերիշխող պրակտիկան է»*: Krasner, Stephen “Introduction” // Stephen D. Krasner (ed.) International Regimes, Ithaca, N.Y.: Cornell University Press, 1983.

3. Տերմինաբանական խառնաշփոթն ավելի է խորանում միջազգային կազմակերպությունների կողմից «կառավարում» բառի տարբեր իմաստներով կիրառելու արդյունքում: Օրինակ՝ «պատշաճ կառավարում» (good governance) տերմինն օգտագործվում է թափանցիկության հասնելու, չինովնիկների գործունեության արդյունավետության բարձրացմանն ու կոռուպցիայի նվազմանն ուղղված պետական աշխատակազմի բարեփոխումների վերաբերյալ Համաշխարհային բանկի ծրագրերում: Այս համատեքստում «կառավարում» տերմինն անմիջականորեն կապված էր կառավարության հիմնական գործառույթների հետ:

4. Shannon, Victoria. “What’s in an ‘i’? Internet Governance” // International Herald Tribune, 3.12.2006 (համացանցային հասցեն՝ http://www.iht.com/articles/2006/12/03/technology/btitu. php).

5. Ժնևի WSIS փուլին նախապատրաստվելու ընթացքում «համացանց» տերմինի կիրառումների զարգացման մասին տես՝ DiploFoundation. The Emerging Language of ICT Diplomacy – Key Words (համացանցային հասցեն՝ http://www.diplomacy.edu/IS/Language/html/words.htm).

6.Ֆոլկեր Կիթցը ապացույցներ է բերում հօգուտ հեռախոսակապի համակարգի և համացանցի հասցեների ու անունների ծավալի միջև համանմանության օրինաչափության: Տես՝ *Volker Kitz (2004). ICANN May Be the Only Game in Town, But Marina del Rey Isn’t the Only Town on Earth: Some Th oughts on the So-Called “Uniqueness” of the Internet* (համացանցի հասցեն՝ http://www.smu.edu/csr/articles/2004/Winter/Kitz.pdf):

7. 2008 թ. նոյեմբերի 6-ին Կահիրեում ICANN համաժողովի ընթացքում արտասանած ելույթներից մեջբերումներ (համացանցային հասցեն՝ https://cai.icann.org/fi les/meetings/cairo2008/toure-speech-06nov08.txt):

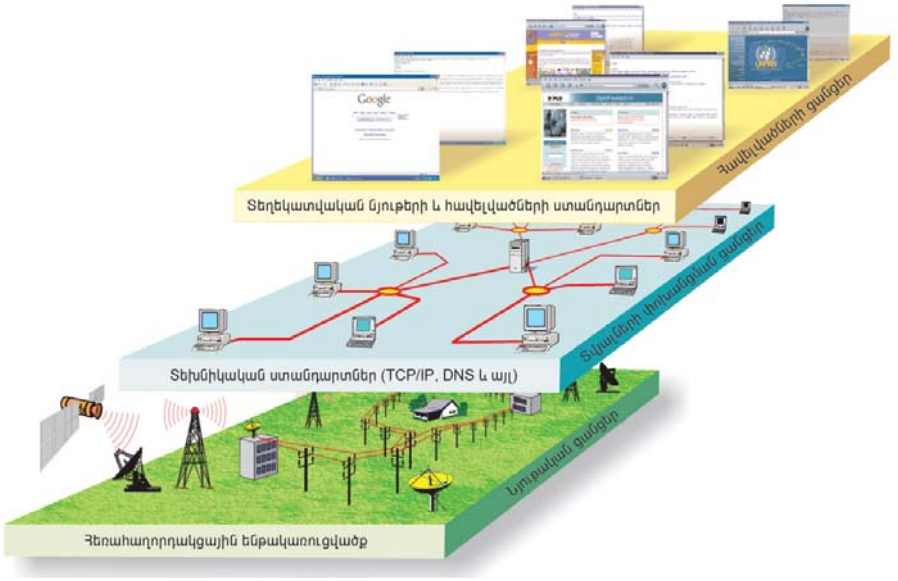
8. Գրքում մեջբերված համացանց-ռեսուրսների մասին բոլոր հղումները ստուգվել են 2008 թ. նոյեմբերի 14-ին:

Բաժին 2

Ենթակառուցվածք և ստանդարտացում

Ենթակառուցվածք և ստանդարտացում

Ենթակառուցվածք և ստանդարտացում զամբյուղն ընդգրկում է համացանցի գործառույթների հետ կապված, հիմնականում, տեխնիկական հարցեր: Զամբյուղին այս կամ այն հարցի վերաբերման հիմնական չափանիշը դրա կարևորությունն է՝ համացանցի բազային տեխնիկական գործառնությունների տեսակետից:
Այս զամբյուղին վերաբերող հիմնախնդիրները կարելի է բաժանել երկու խմբի: Առաջին խումբը ներառում է առավել կարևոր հարցեր, առանց որոնց լուծման ոչ համացանցը, ոչ «համաշխարհային սարդոստայնը» (WWW) չեն կարող գոյություն ունենալ[1]: Այդ խումբը ներկայացված է հետևյալ երեք մակարդակով կամ շերտով՝



1) հեռահաղորդակցային ենթակառուցվածք, որի միջոցով փոխանցվում է համացանցային տվյալների հոսքը (թրաֆիկը),
2) տեխնիկական ստանդարտներ և ծառայություններ՝ ենթակառուցվածք, որի շնորհիվ համացանցն աշխատում է (օրինակ՝ TCP/IP, DNS, SSL),
3) նյութերի բովանդակության (կոնտենտի) և ներդիրների (օրինակ՝ HTML, XML) ստանդարտները:
Հիմնախնդիրների երկրորդ խումբն ընդգրկում է համացանցի ենթակառուցվածքի կայուն և անվտանգ գործառույթների ապահովման հետ կապված հարցերն ու ներգրավում է կիբեռանվտանգության, տվյալների գաղտնագրման և փոստաղբի դեմ պայքարի հիմնախնդիրները:

Հեռահաղորդակցության ենթակառուցվածք

Արդի վիճակ

Համացանցի տվյալների հոսքը կարող է փոխանցվել ամենատարբեր կրողների՝ հեռախոսալարերի, մանրաթելային մալուխի, գերկարճալիք ազդանշանների և անլար կապի օգնությամբ: Համացանց-թրաֆիկի փոխանցման համար կարող է օգտագործվել նույնիսկ ամենասովորական էլեկտրական ցանցը[2]: Քանի որ համացանց-թրաֆիկի հաղորդումները հիմնվում են հեռահաղորդակցությունների մակարդակի վրա, ապա այդ ոլորտի կարգավորման ամեն մի նոր միջոց անխուսափելիորեն ազդում է նաև համացանցի վրա: Հեռահաղորդակցության ենթակառուցվածքը կարգավորում են մի շարք պետական և մասնավոր կազմակերպություններ ինչպես ազգային, այնպես էլ միջազգային մակարդակով:
Հեռահաղորդակցությունների կարգավորման բնագավառում միջազգային հիմնական կազմակերպություններից են, օրինակ՝ Հեռահաղորդակցության միջազգային միությունը (ՀՄՄ), որը մանրամասն մշակել է կանոններ, որոնք կարգավորում են ազգային օպերատորների միջև հարաբերությունները, ռադիոհաճախականության բաշխումը և արբանյակների դիրքը, ինչպես նաև Առեւտրի համաշխարհային կազմակերպությունը (ԱՀԿ), որը կարևորագույն դեր է խաղում ողջ աշխարհում հեռահաղորդակցության շուկաների ազատականացման գործում[3]: Սակայն ԱՀԿ-ի և ՀՄՄ-ի դերերը էականորեն տարբերվում են: ՀՄՄ-ն հաստատում է մանրամասն մշակված տեխնիկական ստանդարտներ, միջազգայնորեն սահմանված կարգեր,

ՀՄՄ միջազգային կանոնակարգը

1988 թ. ՀՄՄ-ի նախապատրաստած միջազգային հեռահաղորդակցության կանոնակարգը նպաստեց ծառայությունների և գնագոյացման միջազգային ազատականացմանը, նաև հնարավոր դարձրեց այնպիսի բազային ծառայությունների ներդրումային օգտագործումն, ինչպիսին ուղիների միջազգային վարձակալությունն է: Այսպիսով, համացանցի արագ զարգացման համար 1990-ականներին ստեղծվեց ենթակառուցվածքային բազա:

որոնք անմիջականորեն վերաբերում են հեռահաղորդակցություններին, և օգնություն է ցուցաբերում զարգացող երկրներին[4]: ԱՀԿ-ն առաջադրում է շուկայի ընդհանուր կանոնների շրջանակներ[5]: Հեռահաղորդակցությունների ազգային շուկաների ազատականացումը այդ բնագավառի խոշորագույն ընկերություններին (AT&T, Cable and Wireless, France Telecom, Sprint, WorldCom) հնարավորություն է տվել իրենց շուկաները գլոբալ ընդլայնելու: Քանի որ համացանց-թրաֆիկի հիմնական մասը այդ ընկերություններին պատկանող կապի միջոցներով է փոխանցվում, ապա դրանք զգալի ազդեցություն են ունենում համացանցի զարգացման գործում:

Հարցեր

«Վերջին մղոնը»՝ կապի տեղական ուղիներ

«Վերջին մղոն» (կամ անգլերեն՝ local loop) է կոչվում համացանցի ծառայություններ մատակարարող ընկերության (պրովայդերի) և վերջին օգտատերի միջև եղած կապուղին: Տեղական կապուղիների հետ ունեցած հիմնախնդիրները խոչընդոտ են դառնում շատ երկրներում (հաճախ զարգացող երկրներում) համացանցի ավելի լայն տարածման համար: «Վերջին մղոն» հիմնախնդրի ոչ թանկ արժեցող հավանական լուծումներից մեկը կարող է դառնալ անլար կապի կիրառումը: Բացի նոր տեխնոլոգիաներից, որոնք ավելի ու ավելի հասանելի են դառնում, տեղական կապուղիների հիմնախնդրի լուծումը նույնպես կախված է հեռահաղորդակցությունների շուկայի այդ հատվածի ազատականացումից:

Հեռահաղորդակցությունների շուկայի ազատականացում

Կապի ծառայությունների տեղական շուկաները շատ երկրներում են ազատականացված: Սակայն շատ զարգացող երկրներ, որտեղ իշխանությունները տիրում են հեռահաղորդակցության ծառայությունների մենաշնորհին, բախվել են մի բարդ խնդրի՝ ինչպես ազատականացնել կապի ծառայությունների շուկան և այն ավելի արդյունավետ դարձնել, միևնույն ժամանակ պահպանել հեռահաղորդակցությունների մենաշնորհից ստացվող բյուջեի մուտքերի կարևորագույն աղբյուրը[6]: Միջազգային օգնությունը, աստիճանաբար կատարվող բարեփոխումները և ազատականացման գործընթացի համաձայնեցվածությունը հասարակական շահերի պաշտպանության հետ կարող են օգնել դուրս գալու այս իրավիճակից:

Ենթակառուցվածքի տեխնիկական ստանդարտների հաստատումը

Մասնավոր ու արհեստավարժ ինստիտուտներն ավելի ու ավելի շատ են հաստատում տեխնիկական ստանդարտներ: Օրինակ՝ անլար կապի ստանդարտը (WiFi) IEEE 802.11b մշակել են էլեկտրատեխնիկայի և էլեկտրոնիկայի (IEEE) ինստիտուտի ինժեներները: WiFi ստանդարտի հետ համատեղելի սարքավորումների հավաստագրումն իրականացնում

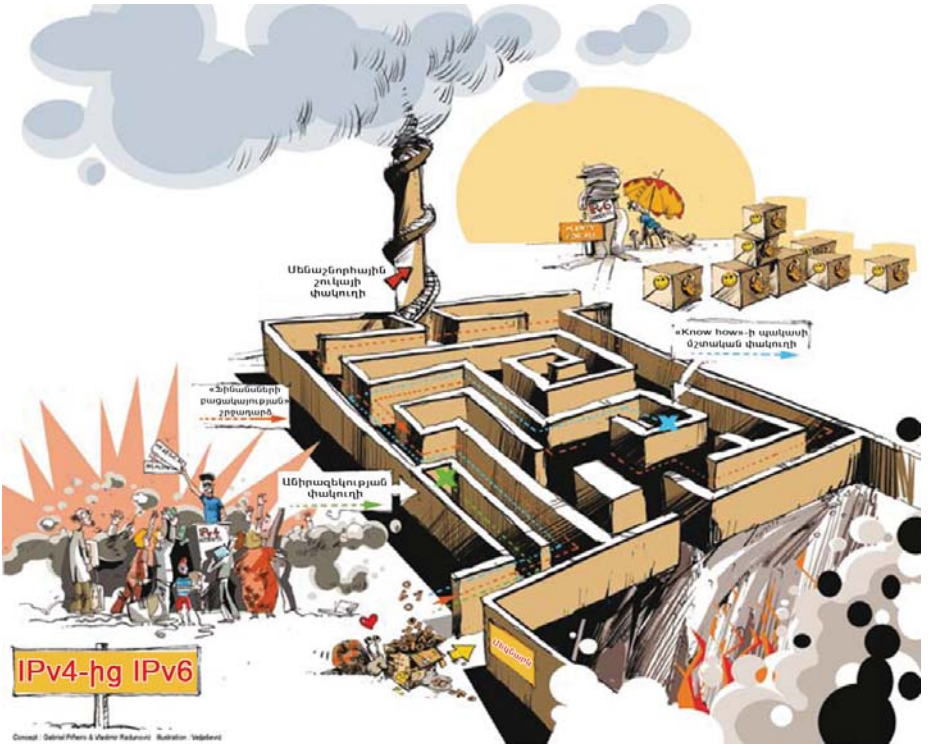
է WiFi Alliance կազմակերպությունը: Այդ ինստիտուտների դերն ինքնին, հատկապես այդքան արագ զարգացող շուկայում ստանդարտների հաստատումն ու ներդրումը, նրանց հնարավորություն է տալիս զգալի ազդեցություն ունենալ շուկայի վրա:

Փոխանցումների կառավարման արձանագրություն/ Համացանց-արձանագրություն (TCP/IP)

Արդի վիճակը

TCP/IP-ը այն հիմնական տեխնիկական ստանդարտն է, որը սահմանում է համացանցի միջոցով տվյալների փոխանցման եղանակը: Այս արձանագրությունը հիմնված է երեք սկզբունքի վրա՝ փաթեթային կոմուտացիա, տվյալների համընդգրկուն փոխանցում և խոչընդոտների դեմ կայունություն: TCP/IP արձանագրության հետ կապված համացանցի կառավարման հարցերում կարելի է երկու ուղղություն առանձնացնել՝ ա) նոր ստանդարտների ներդրում, բ) IP հասցեների բաշխում: TCP/IP-ի համար ստանդարտները սահմանում են համացանցի նախագծման հարցերով զբաղվող աշխատանքային խումբը (IETF): Քանի որ այդ արձանագրությունը համացանցի գործառույթների համար սկզբունքային նշանակություն ունի, այն խստորեն պահպանվում է IETF-ում: TCP/IP արձանագրության մեջ մտցված յուրաքանչյուր փոփոխություն նախապես բազմակողմանի քննարկման և ընթացիկ հիմնախնդիրների լուծման համար դրանց արդյունավետության հաստատման («աշխատող կոդի» սկզբունքը) կարիք ունի:

IP հասցեները թվային հասցեներ են, որոնք ցանցին միացած բոլոր համակարգիչները պետք է ունենան: Այդ հասցեները եզակի են՝ համացանցին միացած երկու համակարգիչ չեն կարող ունենալ միանման IP հասցե: Դա էլ հասցեները դարձնում է հնարավոր դեֆիցիտային ռեսուրս: IP հասցեների բաշխման համակարգը կազմակերպված է ստորակարգությամբ: «Վերևում» գտնվում է համացանցում անունների շնորհման վարչությունը (Internet Assigned Numbers Authority, IANA), որը ICANN-ի դուստր կառույցն է: IANA-ն IP հասցեների բլոկները բաշխում է տարածաշրջանային հինգ համացանցային մատենավարությունների միջև[7]: Տարածաշրջանային համացանցային մատենավարություններն, իրենց հերթին, հասցեները բաժանում են ազգային ու տեղական համացանցային մատենավարությունների միջև, իսկ դրանք IP հասցեները փոխանցում են ավելի ցածր աստիճանի, համացանցային ոչ մեծ ծառայություններ մատուցողներին, ընկերություններին և մասնավոր անձանց:



Հարցեր

IP հասցեների սահմանափակ լինելն ինչպես հաղթահարել. անցում IPv6 արձանագրությանը

Այսօր IPv4-ը (4-րդ վերսիայի համացանցային արձանագրությունը) կիրառելիս IP հասցեների ընդհանուր քանակը կազմում է մոտավորապես 4 միլիարդ և կարող է սպառվել մոտակա մի քանի տարվա ընթացքում՝ համացանցին միացվող նոր սարքավորումների ի հայտ գալու արդյունքում, ինչպիսիք են, օրինակ՝ բջջային հեռախոսները, գրպանի համակարգիչները, խաղային կցորդները և կենցաղային էլեկտրասարքավորումները:
Մտահոգությունն այն մասին, որ IP հասցեները կարող են վերջանալ (ինչը կարող է խոչընդոտել համացանցի հետագա զարգացմանը), տեխնիկական միությանը ստիպել է նախաձեռնել հետևյալ կարևորագույն քայլերը.
- IP հասցեների գոյություն ունեցող պաշարների ռացիոնալ օգտագործում, ինչը հասանելի դարձավ ի հաշիվ ցանցային հասցեների (NAT) վերափոխման տեխնոլոգիայի կիրառման.
-առանց դասակարգման հասցեավորման (Classless InterDomain Routing, IDR) մեխանիզմի արմատավորում, որի նպատակն է դադարեցնել տարածաշրջանային մատենավարություններում IP հասցեների շռայլ բաշխումը.

-համացանցային արձանագրության նոր վերսիայի՝ IPv6-ի ներդրումը, որն IP հասցեների ավելի մեծ պաշար է տրամադրում (430 000 000 000 000 000 000 000):

IP հասցեների հավանական սպառման հիմնախնդրին առնչվող տեխնիկական համացանցային միության գործողություններն իրավիճակն արագ և նախազգուշական կառավարման օրինակ են: NAT և CIDR տեխնոլոգիաները հնարավորություն տվեցին հաղթահարելու ընթացիկ բարդությունները, սակայն լավագույն երկարաժամկետ լուծումը արձանագրության նոր՝ IPv6 վերսիային անցնելն է: IPv6-ն մշակվել է դեռևս 1996 թ., սակայն դրա ներդրումը շատ դանդաղ է ընթանում: Քանի որ IPv4 արձանագրության վերսիայում մատչելի IP հասցեները 2011 թ. լրիվ կսպառվեն, ապա այդպիսի դանդաղ անցումը արձանագրության նոր վերսիային սպառնում է իսկական ճգնաժամ ստեղծել: IPv6-ի ներդրման ընթացքում հիմնական բարդություններից մեկը IPv6 և IPv4 վերսիաների միջև հետադարձ ոչ բավարար համատեղելիությունն է: IPv6 օգտագործող ցանցերը չեն կարող ուղղակիորեն համագործակցել IPv4 օգտագործող ցանցերի հետ, որոնք այսօր մեծամասնություն են: Քանի որ մեծ է այն բանի հավանականությունը, որ IPv4 և IPv6 վերսիաներն օգտագործող ցանցերը ապագայում պետք է համագոյակցեն, ապա շատ կարևոր է ապահովել նոր IPv6 ցանցերի մատչելիությունը, որպեսզի դրանք չմնան մեկուսացած «կղզիներ»: Հիմնախնդրի տեխնիկական լուծումը ենթադրում է երկու տեսակի ցանցերի միջև հատուկ «թունելի» ստեղծում, ինչը կբարդացնի համացանցում (շրջելու)երթևեկման համակարգը, ինչպես նաև զուգընթաց կառաջացնի մի շարք հիմնախնդիրներ: Ներդրումը հետաձգվում է նաև համացանցային ծառայություններ մատուցողների (պրովայդերների) և օգտատերերի հետաքրքրության բացակայության պատճառով: Թեև նրանց քաջ հայտնի է IP հասցեների սպառման վտանգի մասին, այնուամենայնիվ նրանք նախընտրում են գործել «կապրենք՝ կտեսնենք» սկզբունքով: Օրինակ՝ Ճապոնիայում վերջին ժամանակներում անցկացրած հետազոտությունների արդյունքները ցույց են տալիս, որ թեև համացանցային ծառայություններ մատուցողների 70 տոկոսը գիտի IPv4 արձանագրության վերսիայում IP հասցեների սպառման վտանգի մասին, սակայն նրանցից միայն 30 տոկոսն է պատրաստվում անցում կատարել IPv6-ի:

Այնպիսի իրավիճակներում, երբ հիմնախնդիրը շուկայական մեխանիզմների հիման վրա լուծում չի գտնում, անհրաժեշտություն է առաջանում, որպեսզի կառավարություններն ու պետական իշխանության այլ մարմիններն ավելի ակտիվորեն աջակցեն IPv6-ին անցմանը՝ տարածելով IP հասցեների սպառման մասին տեղեկատվություն, IPv6 վերսիային անցնելու և IPv6 կառավարական ցանցերում կիրառելու գործում ֆինանսական աջակցություն ցուցաբերելով: Ուշադրության արժանացնելով IPv6-ին անցնելու բարդությունը, զարգացող՝ հիմնականում աֆրիկյան երկրները կարող են օգուտ ստանալ ուշ տեղ հասած տեղեկատվականացումից և ի

Տեխնոլոգիաներ, ստանդարտներ և քաղաքականություն

Ցանցային արձանագրությունների մասին բանավեճերը ցույց են տալիս, թե ինչպես կարող են ստանդարտները «այլ միջոցներով քաղաքականություն» լինել: Կառավարության միջամտությունը բիզնեսի և տեխնոլոգիայի հարցերին (օրինակ՝ անվտանգության կամ հակամենաշնորհային գործունեություն ծավալելը) սովորաբար ընկալվում է որպես քաղաքական և հասարակական նշանակություն ունեցող երևույթ, միևնույն ժամանակ տեխնիկական ստանդարտները սովորաբար համարվում են սոցիալապես չեզոք, այդ պատճառով էլ պատմության համար հետաքրքրություն չներկայացնող երևույթ: Սակայն տեխնիկական որոշումները կարող են ունենալ հեռուն գնացող տնտեսական ու սոցիալական հետևանքներ, փոխելով մրցակից ֆիրմաների կամ երկրների միջև ուժերի հավասարակշռությունը և սահմանափակելով օգտատերերի ազատությունը: Պաշտոնական ստանդարտներ հաստատելու փորձերը հասարակական դաշտ են հանում այս կամ այն համակարգի մշակողների տեխնիկական մասնակի լուծումները: Այդպիսով, ստանդարտների պատճառով առաջացած «մարտերը» կարող են ի հայտ բերել շահերի ակնկալիքներով թաքուն հույսեր և բախումներ: Իսկ այն ավյունը, որով շահագրգիռ կողմերը վիճաբանում են ստանդարտների վերաբերյալ այս կամ այն որոշումների առիթով, մենք համարում ենք նշան այն բանի, որ զուտ տեխնիկական որոշումների հետևում ավելի խորը իմաստ է թաքնվում: Աղբյուրը՝ Janet Abbate. Inventing the Internet. MIT Press, 1999.

սկզբանե IPv6-ի վրա հիմված ցանցեր ներմուծելու հնարավորությունից: Ներդրման ընթացքում զարգացող երկրներին տեխնիկական օգնություն ցուցաբերելու անհրաժեշտություն է լինելու[8]: IPv6-ին անցնելու ուղղությամբ գործողությունների քաղաքական ծրագիրն, ըստ էության, արձանագրության նոր վերսիային փոխադրվելու հիմնախնդրից բացի, պետք է լուծի IP հասցեների արդարացի բաշխման խնդիրը, որի համար անհրաժեշտ է ներդնել վերջին օգտատերերի պահանջները լավագույնս բավարարող մրցակցային նոր մեխանիզմներ:

Փոփոխություններ համացանցային արձանագրություններում և կիբեռանվտանգություն

Համացանցի առաջին մշակողների համար անվտանգությունը կարևորագույն հարցերից չէր, քանի որ այն ժամանակ համացանցը գիտահետազոտական ինստիտուտների փակ ցանցից էր կազմված: Համացանցի գլոբալ տարածումն ու աճող առևտրային նշանակությունը հանգեցրին այն բանին, որ անվտանգության հարցերը դարձան համացանցի կառավարման հիմնախնդրի առաջնային հարցերից մեկը: Քանի որ համացանցի կառույցը ստեղծվել էր առանց հաշվի առնելու կիբեռանվտանգության հարցերը, ապա դրանում համապատասխան գործիքների ներկառուցումը կպահանջի համացանցի, TCP/IP արձանագրության հիմքում էական փոփոխություններ կատարել: Նոր IPv6 արձանագրությունը անվտանգության տեսակետից նախատեսում է մի քանի բարելավում, սակայն, միևնույն է, դա լիարժեք լուծում չէ: Այդպիսի պաշտպանվածության ապահովումը պահանջում է էական TCP/IP վերափոխում[9]:

TCP/IP փոփոխությունը և անցագրային սահմանափակ ունակության հիմնախնդիրը

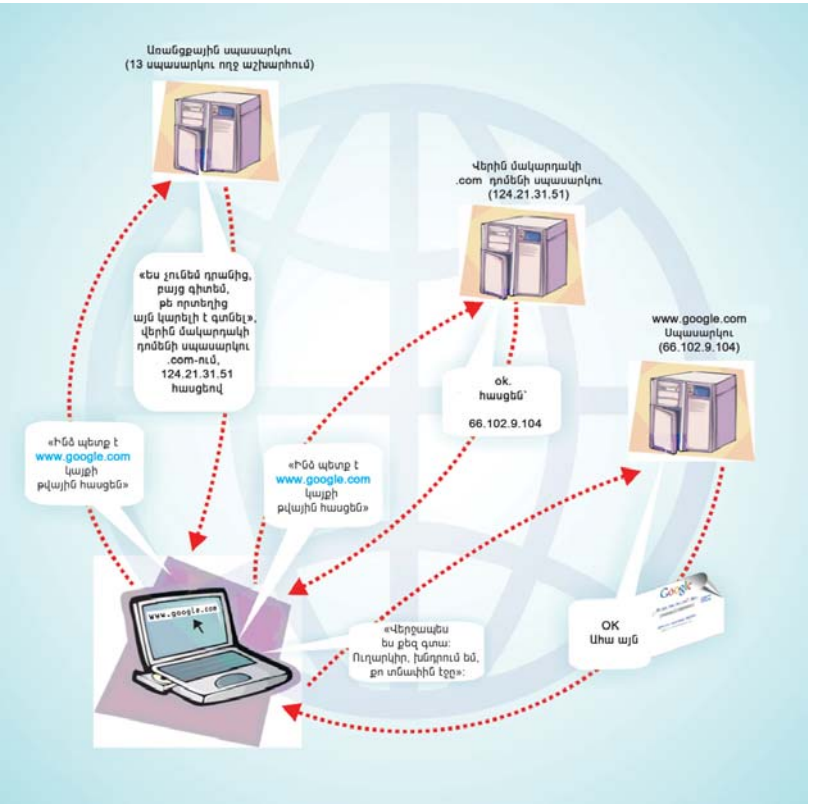
Համացանցի միջոցով մուլտիմեդիական նյութերի փոխանցումը հեշտացնելու համար (օրինակ՝ ձայնային կապի կամ «հարցման վերաբերյալ տեսանյութ») անհրաժեշտ է ապահովել օգտագործման ցուցանիշների որոշակի նվազագույն մակարդակ երաշխավորող ծառայությունների որակը: Դա կարևոր է, հատկապես, ներդիրների համար, որոնց դեպքում ուշացումն անթույլատրելի է, օրինակ՝ իրական ժամանակակարգով հաղորդում փոխանցելիս: Հիմնական խնդիրը համացանցային ուղիների անբավարար անցագրային ունակությունն է: Ծառայությունների որակի ապահովումը կարող է փոփոխություններ պահանջել համացանցային արձանագրություններում, ընդհուպ ցանցային չեզոքության սկզբունքից հրաժարումը:

Դոմենային անունների համակարգը (DNS)

Արդի վիճակը

Դոմենային անունների համակարգն (DNS) աշխատում է համացանցային հասցեների հետ (օրինակ՝ www.google.com) և դրանք վերածում է IP-հասցեների (պարզեցված գծագիրը պատկերված է ստորև՝ նկարում): DNS-ը կազմված է «արմատական» սպասարկուներից, վերին մակարդակի դոմենային սպասարկուներից և աշխարհի տարբեր ծայրերում տեղակայված բազում DNS սպասարկուներից:

Համացանցի կառավարման վերաբերյալ քննարկումների ընթացքում դոմենային անունների համակարգի կառավարումը միշտ բուռն վեճերի առարկա է եղել: Առավել հակասական հանգամանքներից մեկը արմատական սպասարկուների՝ ստորակարգությամբ կազմակերպված դոմենային անունների համակարգի ամենաբարձր աստիճանի վրա ԱՄՆ կառավարության հսկողությունն է (առևտրի նախարարության միջոցով): Իրավիճակն ավելի սրում է այն փաստը, որ գոյություն ունեցող 13 արմատական սպասարկուներից 10 գտնվում է ԱՄՆ-ում (մյուս 3-ը տեղակայված են Եվրոպայում և Ասիայում): Այս հիմնախնդիրը լուծելու և դոմենային անունների մասշտաբայնությունը ապահովելու համար մշակվել էր «Anycast» տեխնոլոգիան, որն այսօր ներառում է աշխարհով մեկ բոլոր մայրցամաքներում տարածված ավելի քան հարյուր սպասարկուների: DNS-ը ներառում է բարձր մակարդակի դոմենների երկու տեսակ: Առաջին տեսակն, այսպես կոչված, շարքային (կամ «ընդհանուր») դոմեններն են, երկրորդը՝ երկրների կոդերի վրա հիմնված դոմենները: Ծնունդ առած յուրաքանչյուր բարձր աստիճանի դոմենի (generic top-level domain, gTLD) համար հասցեների ցուցակը պահում է մեկ մատենավարություն: Օրինակ՝ .com դոմենի վարչարարությունն իրականացնում է VeriSign ընկերությունը: «Վաճառողի» գործը ստանձնում են մատենավարները:



ICANN-ը (Համացանցում հասցեներ և անուններ շնորհող կորպորացիան) կոորդինացնում է DNS ընդհանուր համակարգը, ներառյալ համաձայնագրերը և մատենավարություններին ու մատենավարներին տալիս է հավատարմագրեր: Այդ կազմակերպությունը սահմանում է այն մեծածախ գինը, որով արձանագրման բաժինը (օրինակ՝ VeriSign-ը) վարձակալությամբ արձանագրողներին տալիս է դոմենային անուններ և հաստատում է արձանագրողների ու արձանագրման բաժինների ծառայություններ մատուցելու որոշակի պայմանները: Այդպիսով, ICANN-ը բարձր աստիճանի դոմենային անունների շուկայում գործում է որպես տնտեսական և իրավական հարցերը կարգավորող մարմին: Դոմենային անունների համակարգի կառավարման կարևոր մասն է առևտրային վճարանիշերի պաշտպանությունն ու վեճերի լուծումը: Համացանցի արշալույսին դոմենային անունների գրանցումը հիմնված էր. «ով առաջինն է գալիս, նրան առաջինն են սպասարկում» սկզբունքի վրա, ինչի արդյունքում ծնունդ է առնում դոմենային անունների ձեռքբերման երևույթը (cybersquatting), որի նպատակը դրանց հետագա վերավաճառքն էր: ICANN-ի և Մտավոր սեփականության համաշխարհային կազմակերպության

(WIPO) մշակած դոմենային անունների վերաբերյալ վեճերի քննարկման միասնական քաղաքականությունն օգնեց էականորեն կրճատել դոմենային անունների ձեռքբերման երևույթը: DNS կառավարման գոյություն ունեցող կառուցվածքի մեկ այլ կարևոր բաղադրիչ է ազգային բարձր աստիճանի դոմենների կառավարումը (country code top-level domains, ccTLDs): Ներկայում դրանցից շատերը գտնվում են ոչ պետական ինստիտուտների և մասնավոր անձանց վերահսկողության ներքո, որոնք այդ իրավունքն ստացել էին համացանցի զարգացման սկզբնական փուլում, երբ կառավարություններն այդպիսի հարցերով չէին հետաքրքրվում:

Հարցեր

Դոմենային նոր անունների ստեղծումը

Տեխնիկական տեսակետից դիտարկելիս, դոմենային վերին մակարդակի անուններ (gTLDs) ստեղծելու հնարավորությունները, գործնականորեն, սահմանափակ չեն: Սակայն մինչ օրս դոմենային նոր գոտիների ներդրումը շատ դանդաղ էր ընթանում. միայն վերջերս ստեղծվեցին մի քանի նոր gTLD-ներ: Ներկայում գոյություն ունի 20 gTLD և քննարկվում է ևս երեքը ստեղծելու հնարավորությունը[10]: Նոր gTLD-եր ներդնելու դեմ հիմնականում դիմադրություն են ցուցաբերում առևտրային ընկերությունները, որոնց անհանգստացնում է այն փաստը, որ դոմենների թվի ավելացումը կարող է բարդացնել առևտրային ապրանքանիշերի պաշտպանության հիմնախնդիրը: ICANN-ը քննելով գործադրվող ճնշումները՝ վերին մակարդակի դոմենային նոր անունների ստեղծման հարցում, խորհրդատվությունների գործընթաց սկսեց, որն ուղղված էր այդ ոլորտում նոր քաղաքականության մշակմանը: Այդ քաղաքականությունն, ամեն ինչից զատ, կոչված է լուծելու դոմենային անունների, հասարակական բարոյականության, ինչպես նաև գրանցման արժեքի վերաբերյալ վեճերի կարգավորման խնդիրը: Վերին մակարդակի դոմենային անունների նկատմամբ նոր քաղաքականություն պետք է մտցվեր դեռևս 2009 թ.:

Վերին մակարդակի դոմեններ՝ հատուկ տեսակի նյութերի համար

Մեկ այլ քաղաքական հիմնախնդիր, որին բախվել է ICANN-ը, դոմենային նոր գոտիների ստեղծման մասին որոշում ընդունելն էր, որոնց անուններն արտացոլում են դրանցում տեղադրված կայքերի բովանդակության առանձնահատկությունները[11]: Վերջին այդպիսի օրինակը պոռնոգրաֆիկ կայքերի համար .xxx դոմենի ստեղծման մասին առաջարկությունն էր, ինչը ICANN-ի տնօրենների խորհուրդը մերժեց 2007 թ. մարտին: Քննադատները հայտարարեցին, որ ICANN-ն այդ որոշումն ընդունել է ԱՄՆ կառավարության ճնշման տակ, որը կտրականապես դեմ էր .xxx դոմենի ընդունմանը[12]: Հատկանշական է նշել, որ շատ այլ պետություններ այդ հարցում աջակցում էին ԱՄՆ-ին, դրանց թվում էին՝ Չինաստանն ու Բրազիլիան, որոնք,

որպես կանոն, վճռականապես հանդես էին գալիս ընդդեմ համացանցի կառավարման հարցում ԱՄՆ-ի «հատուկ դերի»: Որոշ մարդկանց կարծիքով, .xxx դոմենի ստեղծման հավանական դրական արդյունք կարող էր դառնալ համացանցում «մեծերի համար գոտների» ստեղծումը և կասկածելի նյութեր դիտելու երեխաների հասանելիության թույլտվության սահմանափակումը: Շատ հեղինակներ .xxx դոմենի ստեղծման դեմ հանդես էին գալիս կրոնական և մշակութային պատճառներով: ICANN-ի որոշումը .xxx դոմենի վերաբերյալ թարմացրեց պետական կառավարման հարցերում ICANN-ի դերի մասին բանավեճը:

Վերին մակարդակի դոմենները մշակութային և լեզվական միությունների համար

2003 թ. ICANN-ը որոշում ընդունեց կատալաներեն նյութերի համար նոր՝ .cat դոմեն ստեղծելու մասին: Առաջին անգամ հատուկ դոմեն ստեղծվեց ստույգ լեզվով կայքերի համար[13]: Այդ նախադեպը կարող է նոր հակասությունների հանգեցնել: Նախ՝ հավանական է, որ աշխարհի լեզվական և մշակութային բազմաթիվ միություններ կպահանջեն նույնպիսի արտոնություններ: Երկրորդ՝ մի շարք դեպքերում լեզվական ու կրոնական միությունները ձգտում են ստեղծել սեփական պետությունը, և այդպիսի դոմենի ի հայտ գալը կարող է դառնալ արդեն գոյություն ունեցող երկրների միջև հակասությունների և հակամարտությունների պատճառ: Ինչ վերաբերում է .cat դոմենին, Իսպանիայի կառավարությունը դեմ չարտահայտվեց այդ որոշմանը:

Ազգային դոմենների կառավարումը (ccTLD)

Վերին մակարդակի ազգային դոմենների կառավարումը ներառում է երեք կարևոր հարց: Առաջինը վերաբերում է, մասնավորապես, քաղաքական տեսակետից հակասական այն որոշմանը, թե հատկապես ազգային ինչ կոդեր պետք է գրանցվեն այն դեպքերում, երբ երկրի կամ կազմավորման միջազգային կարգավիճակը պարզ չէ կամ վիճելի է (օրինակ՝ անկախություն նոր ձեռք բերած պետությունները կամ դիմադրության շարժումները): Վերջերս վիճելի հարցերից մեկը Պաղեստինի ինքնավար պետության իշխանությունների գրանցած դոմենային անունն էր: Արդարացնելով դոմենային անունը շնորհելու մասին իր որոշումը, .ps IANA-ն կրկին հայտարարեց ISO 3166 ստանդարտի համաձայն դոմենային անունների գրանցման սկզբունքի մասին, ինչը որ առաջարկում էր համացանցի «հիմնադիր հայրերից» մեկը՝ Ջոն Փոսթելը[14]: Երկրորդ հարցն այն էր, թե ո՞վ պետք է կառավարի ազգային կոդերը: Կառավարություններից շատերը փորձում էին ձեռք բերել սեփական երկրների դոմենների վերահսկողությունը՝ այն համարելով ազգային արժեք: Ընդ որում, պետությունները կիրառում էին քաղաքական տարբեր մոտեցումներ[15]:

Ազգային դոմենի կառավարման իրավունքը նոր ինստիտուտին հանձնումը («վերահանձնումը») ICANN-ը հավանության է արժանացնում միայն

այն դեպքում, եթե երկրի ներսում բոլոր շահագրգիռ կողմերի միջև համաձայնություն է ձեռքբերվում: Հիմնախնդրի մեծ նշանակության և միջազգային մակարդակով այն լուծելու մոտեցումների բազմազանության արդյունքում ներդաշնակության որոշակի մակարդակի հասնելուն ուղղված երկու նախաձեռնություն է անուշադրության մատնվել: Այդպիսի նախաձեռնություններից առաջինը ԿԽԿ սկզբունքներն էին, որոնք հավանության էր արժանացրել ICANN-ի Կառավարական խորհրդատվական կոմիտեն (GAC), որը մշակում է հանձնարարականներ և սահմանում է վերին մակարդակի ազգային դոմենների կառավարման իրավունքի հանձնման գործընթացի վարման ընթացակարգը[16]: Երկրորդ նախաձեռնությունն էր «Լավագույն գործնական մարդիկ», որը 2001 թ. հունիսին մշակել էր Վերին մակարդակի դոմենային անունների համաշխարհային միությունը: Երրորդ հարցը կապված է այն բանի հետ, որ շատ երկրներում դոմենների օպերատորները չեն ցանկանում դառնալ ICANN համակարգի մի մասը: Մինչ օրս ICANN-ին չի հաջողվել ազգային դոմենների օպերատորներին համախմբել «մի տանիքի տակ»: Որոշ դոմենների օպերատորներ ստեղծել են տարածաշրջանային մակարդակի կազմակերպություններ (CENTR-ը՝ Եվրոպայում, AFTLD-ը՝ Աֆրիկայում, APTLD-ը՝ Ասիայում, NATLD-ը՝ Հյուսիսային Ամերիկայում, LACTLD-ը՝ Հարավային Ամերիկայում): Համաշխարհայնացման մակարդակով հիմնական ֆորումը Վերին մակարդակի դոմենների օպերատորների համաշխարհային միությունն է: Ներկայում ICANN-ը վարում է «Հաշվետվության սկզբունքների»՝ ccTLD օպերատորների հետ համագործակցության ավելի պակաս ձևականության մեխանիզմի ստեղծման աշխատանքներ:

Բազմալեզու դոմենային անուններ (IDN)

Համացանցն ի սկզբանե ստեղծվել էր անգլերենով հաղորդակցվելու համար, սակայն շատ արագ վերածվում է հեռահաղորդակցության համաշխարհայնացված միջոցի, ընդ որում, ոչ անգլալեզու օգտատերերի քանակն աճում է: Բազմալեզվության տեսանկյունից համացանցի ենթակառուցվածքի սահմանափակումները կարող են դառնալ ապագայում համաշխարհայնացված (գլոբալ) ցանցի զարգացմանը խոչընդոտող գործոններից մեկը:

IETF-ին կից կազմավորված տեխնիկական միավորումը բազմալեզու դոմենային անունների համար (Internationalised Domain Names, IDN) մշակել է տեխնիկական լուծում, ինչը թույլ է տալիս դրանց անուններում լատինատառերի հետ միասին կիրառել նաև նամակների այլ համակարգեր (օրինակ՝ չինագիր, արաբատառ, կիրիլիցա և այլն): Ներկայում ICANN-ը թեսթավորում է IDN տեխնիկական ապահովման համակարգը: Տեխնիկական դժվարություններից բացի, մեկ այլ, առավել դժվարին հիմնախնդիր է լինելու IDN համակարգի կառավարման քաղաքականության և ընթացակարգի մշակումը: Ավելի ու ավելի ակտիվորեն է զարգանում

այն գաղափարը, որ այդպիսի համակարգի կառավարումը մասառմաս փոխանցվի այն երկրներին կամ երկրների այն խմբին, որտեղ բնակիչները խոսում են մեկ լեզվով: Այսպես, Չինաստանի կառավարությունը մի քանի անգամ մատնանշել է, որ չինարենով IDN համակարգը պետք է կառավարի Չինաստանը: Կիրիլիցաների դոմենների առնչությամբ նույնանման առաջարկով հանդես է եկել Ռուսաստանը: IDN համակարգի կառավարման մշակումն ու քաղաքականության իրականացումը համացանցի կառավարման գործող կարգի հաստատունության համար կծառայի որպես կարևորագույն ստուգումներից մեկը:

1. Կառավարական խորհրդատվական կոմիտեն (GAC) ICANN-ի կառույց է, որը ներկայացնում է պետությունների շահերը և ունի խորհրդակցական լիազորություններ:

«Արմատական» սպասարկուներ

«Արմատական» սպասարկուները, որ գտնվում են դոմենային անունների համակարգի ստորակարգային կառուցվածքի ամենաբարձր գագաթին, մեծ ուշադրություն են գրավում և քննարկման առարկա են դառնում համացանցի կառավարման հարցերով քաղաքական ու գիտական բանավեճերում:

Արդի վիճակ

DNS համակարգի գործառույթներն ու հուսալիությունը վերլուծելու համար քննարկենք շատերին անհանգստացնող մի իրավիճակ, որի դեպքում արմատական սպասարկուները անջատվելու են և համացանցը դադարելու է աշխատել: Նախ՝ գոյություն ունի 13 արմատական սպասարկու, սա տեխնիկական հնարավոր առավելագույն քանակն է: Դրանք բաժանված են ամբողջ աշխարհում (10՝ ԱՄՆ-ում, 3-ը՝ այլ երկրներում. ԱՄՆ-ում 10 սերվերներից մի քանիսը գտնվում են կառավարական գերատեսչությունների տնօրինման ներքո): Եթե սպասարկուներից մեկը շարքից դուրս գա, մյուսների գործունեությունը չի խափանվի: Նույնիսկ եթե 13 սպասարկուն միաժամանակ շարքից գան, ապա դոմենային անունների որոնումը (արմատական սպասարկուների հիմնական գործառույթը) կշարունակվի համացանցով մեկ ստորակարգությամբ բաշխված դոմենային անունների այլ սպասարկուներում[17]: Այլ խոսքով՝ արմատական գոտու ֆայլերի պատճենները պահպանվում են դոմենային անունների հազարավոր սպասարկուներում, ու համացանցի արագ և աղետալի անկումն անհնար է, որ տեղի ունենա: Գործառույթների տեսակետից որևէ լուրջ հետևանք նկատվում է որոշ ժամանակ անց, որի ընթացքում հնարավոր կլինի վերականգնել վնասված սպասարկուները կամ ստեղծել նորերը: Միաժամանակ արմատական սպասարկուների համակարգը էականորեն

ամրապնդում է Anycast տեխնոլոգիան, որն այդ սպասարկուների ողջ պարունակությունը պատճենում է աշխարհով մեկ: Այդպիսի կառուցվածքը շատ առավելություններ է տալիս, ներառյալ DNS համակարգի բարձր հուսալիությունը և համացանցային հասցեներից տեղեկատվությունն առավել արագ ստանալը (Anycast նախագծի շնորհիվ ընտրվում է վերջին օգտատերին ամենամոտ սպասարկուն): 13 արմատական սպասարկուները գտնվում են տարբեր կազմակերպությունների՝ գիտական և հասարակական ինստիտուտների, առևտրային ընկերությունների կառավարական գերատեսչությունների կառավարման ներքո: Արմատական սպասարկուներ կառավարող կազմակերպություններն ստանում են արմատային գոտու ֆայլ, որը նախապատրաստում է համացանցում անունների շնորհման վարչությունը (IANA) և հավանության է արժանացնում ԱՄՆ կառավարությունը (առևտրի նախարարությունը): Առևտրի նախարարությունից համաձայնություն ստանալուց հետո ֆայլի պարունակությունը պատճենահանվում է հիմնական արմատական սպասարկուի վրա, որը առևտրի նախարարության հետ կնքած պայմանագրի համաձայն, գտնվում է VeriSign ընկերության ղեկավարման ներքո: Հիմնական արմատական սպասարկուի ֆայլն այնուհետև ինքնաբերաբար պատճենվում է մյուս բոլոր արմատական սպասարկուների վրա: Այսպիսով, ԱՄՆ կառավարությունը կարող է միակողմանիորեն փոփոխություններ մտցնել DNS համակարգում, ինչը շատ պետությունների մտահոգությունն է առաջացնում:

Հարցեր

Արմատական սպասարկուների վրա սահմանված վերահսկողության ինտերնացիոնալացումը

Շատ երկրներ մտահոգված են ներկայում գոյություն ունեցող սխեմայով, որում արմատական սպասարկուների պարունակության մասին վերջնական որոշումները ընդունում է միայն մեկ պետություն (ԱՄՆ): Համացանցի կառավարման հարցերով բանակցությունների ընթացքում առաջ են քաշվել տարբեր առաջարկներ, այդ թվում նաև «Արմատական սպասարկուների մասին համաձայնագիր» կնքելու գաղափարը (Root Convention), ինչն այդ սպասարկուների քաղաքական վերահսկողությունը կհանձներ միջազգային միությանը կամ, ծայրահեղ դեպքում, պետություններին իրավունք կտար տնօրինելու սեփական ազգային դոմենները: Նոր հեռանկարներ է բացում «Պարտավորությունների հաստատման» ստորագրումը (Affi rmation of Commitments)[18], ինչը կոչված է պայմաններ ստեղծելու ԱՄՆ առևտրի նախարարությունից ICANN-ի ինստիտուցիոնալ անկախության ապահովման և ICANN ապագա ինտերնացիոնալիզացման համար: IANA-ի հետ համաձայնագիրը վերանայվելու է 2011 թ.: Կարելի է առանձնացնել հավանական անցումային վիճակի մի քանի տարր, որը ներառում է երկու փուլ.

- ICANN-ի «Պարտավորությունների հաստատման» բարեփոխման նախաձեռնություն, որի արդյունքում կստեղծվի իր տեսակի մեջ յուրահատուկ միջազգային կազմակերպություն, որն ընդունելի կլինի համացանցի կառավարման ինստիտուցիոնալ ձևի բոլոր պետությունների համար.
-ԱՄՆ առևտրի նախարարությունից արմատական սպասարկուների վերահսկողության հանձնումը ICANN-ին, այն, ինչ առաջարկվում էր ի սկզբանե:

Այլընտրանքային արմատական սպասարկուներ. հնարավորություններ ու սահմանափակումներ

Այլընտրանքային արմատական սպասարկուի ստեղծումը տեխնիկապես բարդ խնդիր չէ: Հիմնական հարցն այն է, թե քանի «հետևորդ» կունենա այլընտրանքային սպասարկուն կամ, ավելի ճիշտ, համացանցում քանի՞ համակարգիչ կդիմի նրան՝ հարցումներով: Այլընտրանքային DNS-ն առանց օգտատերերի իմաստազրկվում է: Այլընտրանքային DNS համակարգ ստեղծելու բազմաթիվ փորձեր են արվել (Open NIC, New.net и Name.space), սակայն դրանց մեծ մասն անհաջողության են մատնվել և գրավել է համացանցի օգտատերերի ընդամենը մի քանի տոկոսին:

Արմատական սպասարկուների կառավարման հարցում ԱՄՆ դերը. ազդեցության տարօրինակությունը

«Պարտավորությունների հաստատումը» փաստաթղթի ընդունումից հետո, արմատական սպասարկուների նկատմամբ ԱՄՆ-ի տարօրինակ ազդեցությունը, հավանաբար, պատմություն կդառնա: Տարօրինակության բուն էությունն այն է, որ «համացանցի քաղաքական քարտեզից» յուրաքանչյուր պետություն ջնջելու հնարավորությունը (տվյալ երկրի բարձր աստիճանի դոմենը հեռացնելով) հազիվ թե ազդեցություն համարվի, քանի որ այն գործնական կիրառություն չունի:
Ազդեցության կարևորագույն տարրը այն հնարավորությունն է, որ ստիպում է մեկ այլ կողմին գործել այդպիսի ազդեցություն ունեցողի կամքին համապատասխան: Համացանցի ենթակառուցվածքում ԱՄՆ-ի «ազդեցության» կիրառումը կարող է անցանկալի հետևանքների հանգեցնել, ընդհուպ երկրների և նույնիսկ տարածաշրջանների համացանցի սեփական այլընտրանքային նախագծերի ստեղծման: Իրադարձությունների այսպիսի զարգացման դեպքում համացանցը կարող է բաժանվել մի քանի չկապակցված մասերի, ինչը վտանգի կենթարկի ԱՄՆ-ի շահերը (ամերիկյան արժեքների գերակշռությունը և անգլերենի՝ որպես համացանցում միջազգային հաղորդակցման լեզվի կարգավիճակը, էլեկտրոնային առևտրի ոլորտում ամերիկյան ընկերությունների իշխող դիրքը): Բ. Օբամայի վարչակազմի առաջին նախաձեռնությունների հիման վրա (օրինակ՝ «Պարտավորությունների հաստատման» ընդունումը) կարելի է եզրակացնել, որ ԱՄՆ-ն գիտակցում է իր իշխանության ողջ տարօրինակությունը. համացանցի կառավարման համաշխարհայնացման ռեժիմի զարգացման ապագայի տեսանկյունից դա կարևոր ազդակ է:

Համացանցային ծառայություններ մատակարարողները

Համացանցային ծառայություններ մատակարարողները (պրովայդերները) համացանցին են միացնում վերջին օգտատերերին: Այդ պատճառով շատ երկրների կառավարությունների տեսակետների համաձայն, դրանք համացանցում իրավական նորմերի պահպանումն ապահովող ամենապարզ ու ակնհայտ մեխանիզմն է: Ըստ համացանցի առևտրային արժեքի աճի և կիբեռանվտանգության հարցերի արդիականացման, շատ պետություններ համացանցային ծառայություններ մատակարարողներին սկսում են օգտագործել որպես իրավակիրառման գործիք:

Հարցեր

Հեռահաղորդակցության մենաշնորհները և համացանցային ծառայություններ մատակարարողները

Այն երկրներում, որտեղ գոյություն ունեն հեռահաղորդակցության մենաշնորհներ, բնորոշ է այնպիսի իրավիճակը, երբ հենց նրանք էլ տրամադրում են համացանց մուտք գործելու իրավունք: Մենաշնորհները խոչընդոտում են համացանցային ծառայություններ մատակարարողների շուկա մուտք գործելուն և թույլ չեն տալիս, որ մրցակցությունը զարգանա: Արդյունքում սահմանվում են չափից ավելի բարձր գներ, ծառայությունների որակը մնում է ցածր, իսկ թվային տեխնոլոգիաներում պառակտվածության հիմնախնդիրը չի լուծվում: Որոշ դեպքերում հեռահաղորդակցային մենաշնորհները հանդուրժում են համացանցային այլ համացանցային ծառայություններ մատակարարողների գոյությունը, սակայն անմիջականորեն միջամտում են նրանց գործունեությանը (օրինակ՝ սահմանափակելով անցագրային ունակությունը կամ արգելքներ ստեղծելով՝ ծառայություններ ցուցաբերելու գործում):

Համացանցային համացանցային ծառայություններ մատակարարողների պատասխանատվությունը հեղինակային իրավունքի տեսանկյունից

Իրավական համակարգերի մեծամասնությունը խոստովանում է, որ համացանցային ծառայություններ մատակարարողները չի կարող պատասխանատվություն կրել հեղինակային իրավունքը խախտող նյութերը տեղադրելու նպատակով իրեն տրամադրած ծառայություններն օգտագործելու համար, եթե չգիտի այդ խախտման մասին: Հիմնական տարբերությունն այն է, թե իրավաբանական ինչ գործողություններ են ձեռնարկվում այն բանից հետո, երբ համացանցային ծառայություններ մատակարարողը տեղեկացված է լինում իր սերվերում տեղադրված նյութերին առնչվող հեղինակային իրավունքի խախտման մասին: Մ.Նահանգների և ԵՄ օրենքները նախատեսում են «նախազգուշացում՝ հեռացում» ընթացակարգը, որի համաձայն համացանցային ծառայություններ մատակարարողը պարտավոր է հեռացնել տվյալ

նյութը, որպեսզի խուսափի դատական հետապնդումից: Ճապոնական օրենսդրությունն ավելի հավասարակշռված մոտեցում է ենթադրում («նախազգուշացում-նախազգուշացում-հեռացում»), որը նյութն օգտագործող անձին իրավունք է տալիս բողոքարկելու կայքից նյութը հանելու մասին պահանջը: Համացանցային ծառայություններ մատակարարողների պատասխանատվությունը սահմանափակող մոտեցումն, ընդհանուր առմամբ, պաշտպանվում է դատական գործով: Ահա մի քանի, դատական առավել նշանակալի նախադեպ, երբ համացանցային ծառայություններ մատակարարողներին ազատել են պատասխանատվությունից՝ մտավոր սեփականության իրավունքները խախտող նյութեր տեղադրելու համար: Դրանցից են՝ սաենտոլոգների գործը (Նիդեռլանդիա), «RIAA-ն ընդդեմ Verizon-ի» գործը (ԱՄՆ), «SOCAN-ն ընդդեմ CAIP-ի» գործը (Կանադա) և «Sabam-ն ընդդեմ Tiscali-ի» գործը (Բելգիա)[19]:

Համացանցում տեղադրվող նյութերի բովանդակությունը վերահսկելու հարցում համացանցային ծառայություններ մատակարարողների դերը

Հասարակական կարծիքի ճնշման ներքո համացանցային ծառայություններ մատակարարողներն աստիճանաբար, թեև ոչ մեծ ցանկությամբ, ներգրավվում են համացանցում նյութերի կարգավորման գործի մեջ: Ընդ որում, նրանք վարքի դրսևորման երկու տարբերակ ունեն: Առաջին՝ հետևել, որպեսզի պահպանվի իշխանության մարմինների մշակած կարգը: Երկրորդը հիմված է ինքնակարգավորման վրա, այսինքն՝ ինքնուրույն որոշել, թե ինչ նյութեր են համապատասխանում համացանցում տեղադրելու համար: Այս տարբերակը կապված է համացանցային ռեսուրսների բովանդակության հանդեպ վարվող քաղաքականությունը « սեփականաշնորհելու» ռիսկի հետ, երբ պրովայդերները կստանձնեն կառավարության գործառույթները:

Փոստաղբի դեմ հակագործողության քաղաքականության մեջ համացանցային ծառայություններ մատակարարողների դերը

Համացանցային ծառայություններ մատակարարողները հաճախ դիտարկվում են որպես փոստաղբի դեմ իրականացվող հակագործողության նախաձեռնությունների հիմնական մասնակիցներ: Սովորաբար համացանցային ծառայություններ մատակարարողներն իրենք են անցկացնում անցանկալի փոստի առաքման ծավալի նվազեցմանն ուղղված միջոցառումներ՝ կիրառելով տվյալների զտման տեխնիկական միջոցները կամ կատարելով փոստաղբի դեմ հակագործողությունների ռազմավարություն: Փոստաղբի վերաբերյալ ՀՄՄ հաշվետվության մեջ նշվում է, որ փոստաղբի տարածման համար պետք է պատասխանատվություն կրեն համացանցային ծառայություններ մատակարարողները և առաջարկվում է ընդունել «Փոստաղբի դեմ հակագործողություններ վարելու օրենք», որը ներառելու է երկու հիմնական դրույթ՝ ա) համացանցային ծառայություններ մատակարարողները պետք է

արգելեն օգտատերերին փոստաղբի առաքումը, բ) համացանցային ծառայություններ մատակարարողները չպետք է տվյալներ փոխանակեն վարքի համապատասխան օրենքը չընդունած այլ ծառայություններ մատակարարողների հետ[20]: Փոստաղբի հիմնախնդիրը նոր բարդություններ է ստեղծում ծառայություններ մատակարարողների համար: Օրինակ՝ փոստաղբի կանխման նպատակով նյութերի զտմանն ուղղված Verizon ընկերության փորձերը մտան դատական գործընթացի մեջ: Verizon-ի զտիչները փոստաղբի հետ միասին ուղեփակեցին նաև թույլատրելի հաղորդագրությունները: Դա անհարմարություններ ստեղծեց այն օգտատերերի համար, ովքեր օրինապահ առաքիչներից նամակների մի մասը չէին ստացել, և արդյունքում Verizon-ին դատի տվեցին[21]:

Լայնագիծ կապի ծառայությունների մեծածախ ծառայություններ մատակարարողները

Համացանց ներթափանցելու կառույցն ունի երեք մակարդակ: Վերջին օգտատերերին միացնող համացանցային ծառայություններ մատակարարողները կազմում են երրորդ մակարդակը: Առաջին և երկրորդ մակարդակները կազմված են լայնաժագիծ կապի ծառայությունների մեծածախ մատակարարներից:

Առաջին մակարդակին տվյալների փոխանցումը իրականացնում են լայնագիծ կապի խոշորագույն ծառայություններ մատակարարողները: Դրանք, որպես կանոն, նույն մակարդակի վրա աշխատող այլ ընկերությունների հետ տվյալների փոխանակման մասին կնքում են, այսպես կոչված, պիրինգային համաձայնագրեր[22]: Առաջին և երկրորդ մակարդակների վրա աշխատող ծառայություններ մատակարարողների միջև եղած հիմնական տարբերությունն այն է, որ առաջինները միմյանց հետ թրաֆիկը փոխանակում են անվճար, պիրինգի սկզբունքով («հավասարը՝ հավասարի հետ»), մինչդեռ երկրորդներն առաջին մակարդակին տվյալներ փոխանցելու համար ստիպված են վճարել համապատասխան ծառայություններ մատակարարողներին[23]: Առաջին մակարդակը սովորաբար վերահսկում են այնպիսի խոշոր ընկերություններ, ինչպիսիք են՝ MCI, AT&T, Cable Wireless и France Telecom: Կապի լայնագիծ ուղիների ոլորտում հեռահաղորդակցության ավանդական ընկերությունները տարածվել են համաշխարհայնացված շուկաներում և համացանցային մայրուղիներում:

Հարցեր

Համացանցային ենթակառուցվածքն, արդյո՞ք, պետք է լինի ընդհանուր օգտագործման ծառայություն

Համացանցային թրաֆիկը կարող է փոխանցվել կապի յուրաքանչյուր ուղով: Սակայն գործնականում որոշակի հզորություններ, օրինակ՝ առաջին մակարդակի մայրուղիները (որոնք, որպես կանոն, օգտագործում են բազմաթել մալուխներ կամ արբանյակային խողովակներ), առանձնահատուկ

կարևոր են համացանցի գործառույթների համար: Համացանցի կառույցում դրանց կենտրոնական դիրքը սեփականատերերին հնարավորություն է տալիս գներ սահմանել և պայմաններ թելադրել իրենց տրամադրած ծառայությունների համար: Վերջին հաշվով, համացանցի գործառնությունը կախված է տվյալների հաղորդման մայրուղիների խողովակների սեփականատերերի ընդունած որոշումներից: Համացանցի օգտատերերի համաշխարհայնացված միությունն, արդյոք, իրավունք ունի՞ խոշորագույն հեռահաղորդակցային օպերատորներից համացանցի կրիտիկական ենթակառուցվածքի հուսալի գործառույթի երաշխիքներ պահանջել: Այդ ընկերություններն, արդյոք, կառավարո՞ւմ են ընդհանուր օգտագործման օբյեկտներ:

Լայնագիծ կապի ծառայություններ մատակարարողները և կրիտիկական ենթակառուցվածքը

2008 թ. սկզբին Եգիպտոսից ոչ հեռու, Միջերկրական ծովում փսասվել էր համացանցային թրաֆիկ հաղորդող հիմնական մալուխներից մեկը: Այդ միջադեպը մի հսկայածավալ տարածաշրջանում՝ մինչև Հնդկաստանի սահմանները, վտանգի ենթարկեց համացանց ներթափանցումը: Նմանատիպ երկու միջադեպ տեղի ունեցավ 2007 թ. (Թայվանի մոտ գտնվող մալուխը և Պակիստան թրաֆիկ հաղորդող հիմնական մալուխը): Այդպիսի իրադարձությունները ցույց են տալիս, որ համացանցի ենթակառուցվածքը ազգային և համաշխարհայնացված կրիտիկական ենթակառուցվածքի մի մասն է: Համացանցային ծառայությունների տրամադրման ժամանակ խափանումները կարող են բացասաբար ազդել տարածաշրջանի տնտեսության և հասարակական կյանքի վրա: Համացանցի աշխատանքի հնարավոր խախտումները մի շարք հարցեր են առաջ քաշում: Արդյոք հուսալի՞ են պաշտպանված համացանցային թրաֆիկ փոխանցող հիմնական մալուխները: Ինչպիսի՞ն է պետություններում կառավարությունների, միջազգային կազմակերպությունների և մասնավոր ընկերությունների դերը մալուխների պաշտպանության գործում: Ինչպե՞ս կարող ենք նվազեցնել համացանցի հիմնական մալուխների հնարավոր փսասվածքների ռիսկերը:

Հեռահաղորդակցությունների ազատականացումն ու հեռահաղորդակցային ծառայություններ մատակարարողների դերը

Գոյություն ունեն հակասական տեսակետներ այն մասին, թե համացանցային ծառայություններ մատակարարողները ու հեռահաղորդակցային ընկերությունները որքան պետք է ենթարկվեն ԱՀԿ (Առեւտրի համաշխարհային կազմակերպություն) կանոններին: Զարգացած երկրներն ապացուցում են, որ հեռահաղորդակցության օպերատորներին ԱՀԿ տրամադրած ազատական կանոնները կարող են վերաբերվել նաև համացանցային ծառայություններ մատակարարողներին: Սահմանափակ

քննարկման կողմնակիցները նշում են, որ ԱՀԿ ռեժիմը կիրառելի է միայն հեռահաղորդակցությունների շուկայի նկատմամբ: Համացանցային ծառայություններ մատակարարողների շուկայի կարգավորումը պահանջում է ԱՀԿ շրջանակներում նոր կանոններ մշակել:

Համացանցին միացումն ապահովող տնտեսական մոդելներ

> *Մենք գիտենք, թե ինչպես կարգավորել փաթեթների փոխանցումը, սակայն չգիտենք, թե ինչպես կարգավորել դոլարների փոխանցումը:*
>
> **Դավիթ Քլարկ**

Արդի վիճակ

Համացանցի կառավարման հարցերի քննարկումը հաճախ շեշտադրում է շահույթի միջոցների և աղբյուրների բաշխման հիմնախնդիրը[24]: Ո՞վ է վճարում համացանցի համար: Համացանցի գործառույթի գործընթացի մեջ ներգրավված տարբեր կողմերի միջև ֆինանսական բազմաթիվ գործողություններ են տեղի ունենում: Անհատ օգտատերերն ու ընկերությունները համացանցի ծառայություններ մատակարարողներին վճարում են համացանց ներթափանցելու և տրամադրվող ծառայությունների համար: Իսկ ինչպես են այդ փողերը բաշխվում համացանց ներթափանցելու ծառայություններ տրամադրող տարբեր ցանցերով մեկ կամ, այլ խոսքով. «փողերն ինչպե՞ս են փոխադրվում համացանցով»[25]: Ահա մի քանի ծախսեր, որոնք ստիպված են ծածկել համացանցի ծառայություններ մատակարարողները (տես՝ նախորդ էջի նկարը).

-համացանցային ծառայություններ մատակարարողները վճարում են կապի օպերատորների ծառայությունների և համացանց ներթափանցելու ուղիների համար,

-համացանցային ծառայություններ մատակարարողները վճարում են տարածաշրջանային կամ տեղական համացանցային գրանցման վայրերին, որոնցից նրանք ստանում են IP հասցեներ՝ հետագա բաշխման համար,

-համացանցային ծառայություններ մատակարարողները վճարում են մատակարարողներին՝ սարքավորումների, ծրագրերով ապահովելու և սպասարկման (ներառյալ կապուղիների գործառույթների, օգնության կենտրոնների և վարչական ծառայությունների համար անհրաժեշտ դիագնոստիկայի գործիքներն ու անձնակազմը) համար,

-դոմենային անուններ գրանցող կազմակերպությունները ծառայությունների համար վճարում են ոչ միայն գրանցողին, այլև IANA-ին,

-կապի օպերատորները վճարում են մալուխներ և արբանյակներ արտադրողներին, ինչպես նաև հեռահաղորդակցային ծառայություններ տրամադրող ընկերություններին: Քանի որ այդ օպերատորները հաճախ

են վարկ վերցնում, ապա նրանք տարբեր բանկերի և կոնսորցիումների տոկոսներ են վճարում:
Այս ցանկը կարելի է շարունակել, սակայն ընդհանուր եզրահանգումը պարզ է. «անվճար ընթրիքներ» չեն լինում: Արդյունքում նշված շղթայի բոլոր ծախսերը վճարվում են համացանցի վերջին օգտատերերի գրպանից, լինեն նրանք անհատներ թե կազմակերպություններ:

Հարցեր

Համացանցի ներթափանցման տնտեսությունն, արդյոք բարեփոխման կարիք ունի՞

Համացանցում տնտեսական ընթացիկ քաղաքականությունն ու փոխազդեցության կարգը ստեղծվել էին դեռևս համացանցի արշալույսին և զարգացման ընթացքում մի քանի փուլ են անցել: Համացանցում տնտեսական փոխազդեցության արդի պրակտիկան կարելի է արդյունավետ համարել, քանի որ շատ դեպքերում այն մատչելի գնով ապահովում է համացանցի կայուն գործառույթը: Տնտեսական ընթացիկ քաղաքականության հիմնական քննադատությունը կապված է երկու տեսակետի հետ՝
-չի բացառվում, որ հիմնական խաղացողները համացանց ներթափանցման ոլորտը մենաշնորհեն, հետևաբար, դրանով իսկ խախտեն ազատ շուկայի գործառույթների սկզբունքները.
-շահույթներն ու ծախսերն անարդար կերպով բաշխվում են համացանցի տնտեսության մասնակիցների միջև:
Ակադեմիական շրջանակներում համացանց ներթափանցման արդար տնտեսության մոդել մշակելու անհամար փորձեր են արվել: Նգուեն և Արմիտրաժը նշում են, որ անհրաժեշտ է համացանցում լավագույն հավասարակշռություն գտնել երեք տարրերի՝ տեխնիկական արդյունավետության, տնտեսական արդյունավետության և հասարակական շահերի միջև[26]: Մյուս հեղինակները նշում են այն դժվարությունները, որոնք ստեղծելու է գոյություն ունեցող պարզ, բոլոր կառույցների համար միանման գնագոյացումից անցումը առավել բարդին՝ կախված փոխանցվող թրաֆիկի ծավալից: Ինչ վերաբերում է փոփոխությունների գործնական արդյունքներին, ապա շատերը գտնում են, որ համացանցում տնտեսական ընթացիկ քաղաքականությունը կարող է բացել «Պանդորայի արկղը»:

Համացանցի ռեսուրսների շուկայում մենաշնորհների ձևավորման անթույլատրելիությունը

Մի քանի մենաշնորհների կլանման շնորհիվ հնարավոր է, որ կարողանան վերահսկել համացանցային թրաֆիկի ամբողջ շուկան[27]:
Այսպիսի հիմնախնդիր գոյություն ունի ինչպես զարգացած, այնպես էլ զարգացող երկրներում: Որոշ հեղինակներ հույս ունեն, որ հեռահաղորդակցային շուկայի ազատականացման գործընթացը կլուծի

մենաշնորհների հիմնախնդիրը (հատկապես գործող օպերատորների նկատմամբ): Սակայն ազատականացումը կարող է հանգեցնել հասարակական մենաշնորհը մասնավոր մենաշնորհով փոխարինմանը: Ջեֆ Հասթոնը պնդում է, որ մենաշնորհի հաստատումն ու համացանցի ռեսուրսների շուկայում բազմազանության կորուստը անխուսափելիորեն կազդեն համացանցի ծառայությունների որակի ու գնի վրա[28]:

Ո՞վ պետք է վճարի զարգացող և զարգացած երկրների միջև կապի համար անհրաժեշտ ծախսերը

«Քենիայից օգտատերը եթե էլեկտրոնային հաղորդագրություն է ուղարկում ԱՄՆ-ի բնակիչ ստացողին, քենիացի համացանցային ծառայություններ մատակարարողները վճարում է ԱՄՆ-ի և Քենիայի միջև միջազգային կապի համար: Սակայն երբ ամերիկացի օգտատերն է էլեկտրոնային հաղորդագրություն ուղարկում Քենիա, միջազգային կապի համար միևնույն է վճարում է քենիացի ծառայություններ մատակարարողը: Արդյունքում քենիացի օգտատերն ավելի բարձր գին է վճարում համացանց ներթափանցելու համար»[29]: Ներկայում զարգացած և զարգացող երկրների միջև տվյալներ հաղորդելու համար վճարում են վերջինները[30]: Ի տարբերություն ավանդական հեռախոսային համակարգի, որում միջազգային յուրաքանչյուր զանգի արժեքը բաժանվում էր երկու երկրների միջև, համացանցում ընդունված մոդելը ողջ բեռը դնում է մեկ կողմի՝ զարգացող երկրների վրա, որոնք պետք է միացվեն առավելապես զարգացած երկրներում տեղակայված մայրուղիներին: Այդպիսով, փոքր ու աղքատ երկրները դրամական օժանդակություն են ցուցաբերում զարգացած երկրների համացանցին: Համացանցի ծառայությունների վճարման գոյություն ունեցող համակարգի փոփոխությունների վերաբերյալ վեճերի հիմնական փաստարկը հեռախոսային ծառայությունների վճարման հետ զուգադրությունն է, որտեղ արժեքը հավասարաչափ բաժանվում է հեռահաղորդակցության վերջնական կետերի միջև: Սակայն Ջեֆ Հասթոնը մատնանշում է, որ այդ զուգադրությունը ոչ մի հիմնավորում չունի: Ավանդական հեռախոսակապի համակարգում գոյություն ունի վճարման ընդամենը մեկ ծառայություն՝ հեռախոսազանգ, որը սեփական հեռախոսների մոտ գտնվող մարդկանց շփման հնարավորություն է տալիս[31]: Համացանցում չի կարելի առանձնացնել միակ «վճարվող ծառայությունը», նրանում միայն տվյալների փաթեթներ կան, որոնք ցանցի ներսում տարբեր ուղիներով են փոխանցվում: Այդ արմատական տարբերությունը վերը նշված զուգադրությունը դարձնում է անկիրարկելի և համացանցի նկատմամբ հեռախոսակապի ծառայությունների համար վճարման մոդելի կիրառման փորձերի դեպքում հիմնական բարդությունների աղբյուրն է: ՀՄՄ-ի նախաձեռնությամբ սկսվել էին բանակցություններ՝ համացանցի ծախսերի վճարման համակարգի հավանական կատարելագործման մասին, որոնց նպատակը համացանց ներթափանցելու արժեքն առավել հավասարաչափ բաշխելն էր: Զարգացած երկրների և հեռահաղորդակցային

օպերատորների հակազդեցության արդյունքում ՀՄՄ-ի ընդունած № D.50 բանաձևը հետևանքներ չունեցավ[32]: Անհաջողության մատնվեցին նաև այդ հիմնախնդիրը ԱՀԿ շրջանակներում քննարկելու փորձերը: Համացանցին միանալու համար վճարման նախագծի կատարելագործման անհրաժեշտության մասին հարցը կրկին վեր հանվեց WSIS-ի ընթացքում և իր արտացոլումը գտավ WGIG հանդիպման հանրագումարային փաստաթղթերի ու հաշվետվության մեջ:

Համացանցային թրաֆիկի փոխանակման կետերի օգտագործման հաշվին համացանց ներթափանցելու արժեքի կրճատումը

Համացանց թրաֆիկի փոխանակման կետերը (Internet Exchange Points, IXP) տեխնիկական ամբողջություն են, որոնց օգնությամբ ծառայություններ մատակարարողները պիրինգի (անվճար) հիման վրա փոխանակում են համացանցային թրաֆիկը: Սովորաբար այդպիսի կետեր ստեղծվում են օգտատերերի սահմանափակ խմբի ներսում թրաֆիկի փոխանակման համար (օրինակ՝ քաղաքի, տարածաշրջանի, երկրի ներսում), որպեսզի խուսափեն աշխարհագրորեն հեռավոր կետերով տվյալների անցանկալի երթուղայնությունից[33]: Համացանցային թրաֆիկի փոխանակման կետերը կարևոր դեր կարող են խաղալ նաև թվային տեխնոլոգիաներում խզումները կրճատելու գործում[34]: Օրինակ՝ եթե երկրում փոխանակման ազգային կետ չկա, ապա անհրաժեշտ է օգտատերերի միջև համացանցային թրաֆիկի զգալի մասն ուղարկել մեկ այլ երկրի միջով: Դա մեծացնում է տվյալների միջազգային փոխանցման ծավալը հեռավոր տարածություններում և համացանցի տրամադրած ծառայությունների արժեքը: Թրաֆիկի փոխանակման ազգային և տարածաշրջանային կետերի ստեղծումը զարգացող երկրների համար կարող է նվազեցնել համացանց ներթափանցելու արժեքը:

«Համաշխարհային սարդոստայնի» (WWW) ստանդարտները

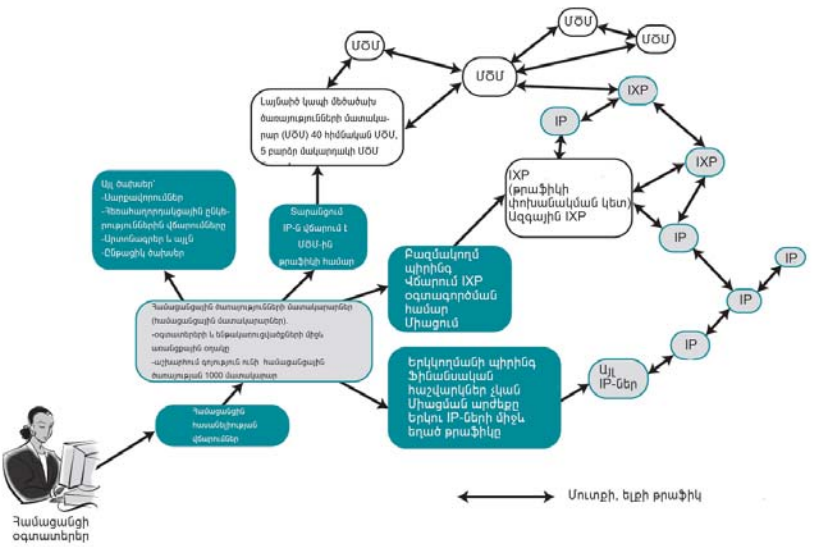
1980-ականների վերջին ցանցային ստանդարտների համար մղվող «ճակատամարտն» ավարտվում է: TCP/IP-ը հետ մղելով մյուսներին, աստիճանաբար դարձավ հիմնական ցանցային արձանագրությունը՝ սատարելով ՀՄՄ X-25 արձանագրությանը (Բաց համակարգերի փոխազդեցության կառույցի մի մասը) և այլ արտոնագրված ծրագրային ապահովման ստանդարտներ, ինչպիսիք են IBM մշակած SNA ստանդարտը: Համացանցը, թեև հեշտացրել էր տարբեր ցանցերի միջև հեռահաղորդակցությունը՝ TCP/IP-ն կիրառելով, սակայն համակարգում դեռևս չկար գործադրման ընդհանուր ստանդարտներ: Դրա լուծումը մշակում են Թիմ Բյոռներս Լին և նրա գործընկերները՝ Ժնևի CERN լաբորատորիայում: Այն համացանցում տեղեկատվության փոխանակման նոր ստանդարտ էր, որ անվանվել է HTML (ըստ էության, գոյություն ունեցող ISO ստանդարտի հեշտացումը, որ կոչվում էր SGML): HTML-ի ի հայտ գալով՝ որպես «համաշխարհային սարդոստայնի» հիմք, համացանցը

սկսեց շեշտակիորեն աճել: HTML-ի առաջին վերսիայի հայտնվելուն պես այդ ստանդարտն անընդհատ թարմացվում ու լրացվում էր նորանոր հնարավորություններով: Մարդու գործունեության տարբեր բնագավառների համար համացանցի աճող կարևորությունը HTML-ի ստանդարտացման հարցը բարձրացրեց: Այն առանձնահատուկ հրատապություն ձեռք բերեց Netscape-ի և Microsoft-ի միջև բրաուզերային պայքարի ժամանակ, երբ ընկերություններից յուրաքանչյուրը HTML ստանդարտի վրա ազդելով, ձգտում է ուժեղացնել իր դիրքը շուկայում: Սկզբում HTML –ը հնարավորություն էր տալիս աշխատելու միայն տեքստերով և նկարներով, սակայն նոր համացանց-հավելվածները տվյալների բազայի կառավարման, տեսանյութերի և անիմացիայի աշխատանքների համար պահանջում էին ավելի բարդ տեխնոլոգիաներ: Հավելվածների այդ բազմազանությունը ստանդարտացման էական ջանքեր էր պահանջում, որպեսզի երաշխավորեր բրաուզերների մեծամասնության միջոցով համացանցում տեղադրվող յուրաքանչյուր նյութի նույնական պատկերումը: Հավելվածների ստանդարտացումը նոր փուլ մտավ XML լեզվի ի հայտ գալով, որը համացանցային էջերի բովանդակման համար ստանդարտների տեղադրման մեծ ճկունություն էր տալիս: Ստեղծվում էին XML ստանդարտների նաև նոր խմբեր: Օրինակ՝ անլար կապով նյութերի տարածման ստանդարտը կոչվում է Wireless Mark-up Language (WML): Հավելվածների ստանդարտացումը առավելապես իրականացվում է «համաշխարհային սարդոստայնի» (W3C) կոնսորցիումի շրջանակներում, որը ղեկավարում է Թիմ Բյոռնս Լին: Հետաքրքիր է, որ համացանցի կառավարման վերաբերյալ քննարկումներում W3C-ը, չնայած համացանցի համար իր մեծ կարևորությանը, դեռևս մեծ ուշադրություն չի գրավում:

«Տվյալների ամպային մշակում»

«Տվյալների ամպային մշակում» («ամպային հաշվարկում») արտահայտությունը կիրառվում է համակարգչային արդյունաբերության նոր միտումները նկարագրելու համար, որոնք որպես համացանցային ծառայություններ ընդգրկված են համակարգչային հավելվածների տրամադրման գործում՝ ի հաշիվ հսկայական «սերվերային ֆերմաների» օգտագործման: Տվյալների ամպոտ մշակման առաջին օրինակները էլեկտրոնային փոստի առցանց ծառայություններն են (Gmail, Yahoo, Hotmail), ինչպես նաև տեքստերի մշակման ակտիվ կապի գործիքները (wiki, Google-ի ծառայությունները): Facebook-ի և նման սոցիալական ցանցերի համար հավելվածների տարածումն արագացրեց «ամպային հաշվարկումների» զարգացումը: Մեր կոշտ սկավառակներից ավելի ու ավելի շատ թվային պաշարներ են փոխադրվում «ամպային» սերվերների վրա: «Տվյալների ամպային մշակման» շուկայում խաղի հիմնական մասնակիցներն են ՝ Google-ը, Microsoft-ը , Apple-ը, Amazon-ը և Facebook-ը, որոնք տիրում են մեծ «սերվերային ֆերմաների»: Տեխնոլոգիաների զարգացումն ուսումնասիրող պատմաբանները կարող են ուշադրություն դարձնել այն բանին, որ «տվյալների ամպային մշակման»

զարգացման հետ շրջանակը փակվել է: Համակարգիչների զարգացման նախնական փուլում կիրառվում էին ընդհանուր օգտագործման հզոր ԷՀՄ-եր («մեյնֆրեյմներ») և ինքնուրույն հաշվողական հնարավորություններ չունեցող օգտատիրական տերմիններ: Հիմնական «միտքը» կենտրոնացած էր կենտրոնական համակարգչի վրա: Հետո, անհատական համակարգիչների և Windows հավելվածների զարգացման շորհիվ հաշվողական հզորությունները տեղափոխվեցին ցանցի վերջին կետետրին: Բոլորաշրջանն, արդյոք, կամփոփվի «տվյալների ամպային մշակման» արդյունքում: Հետագայում, արդյոք, ի հայտ կգան «սերվերային ֆերմաների» մի քանի խոշոր կենտրոնական համակարգիչներ և միլիարդավոր «ոչ բանական» սարքեր, ինչպիսիք են նոութբուքերը, մոնիտորները և բջջային հեռախոսները: Այս և շատ այլ հարցերի պատասխանը ժամանակ է պահանջում: Հիմա մենք կարող ենք անվանել համացանցի կառավարման ընդամենը մի քանի հիմնախնդիրներ, որոնք կծագեն «տվյալների ամպային մշակման» զարգացման արդյունքում: Առաջինն՝ արդի հասարակության կախվածությունը համացանցից աճում է համաձայն այն բանի, թե ինչքան շատ ծառայություններ են հասանելի դառնում առցանց ռեժիմով: Նախկինում առանց համացանցին միանալու մենք չէինք կարող էլեկտրոնային նամակ ուղարկել կամ տեղեկատվությանը հետևել: «Տվյալների ամպոտ մշակման» դարաշրջանում առանց համացանցի անհասանելի կարող է դառնալ նույնիսկ տեքստ գրելը կամ հաշվառում անցկացնելը: Համացանցից աճող այս կախվածությունը կուժեղացնի դրա կայունությունն ու հուսալիությունը ապահովելու կարիքը: Անխուսափելիորեն այն կհանգեցնի համացանցի կառավարման ավելի հզոր ռեժիմի ձևավորմանը, որտեղ առավել ակտիվ դեր են կատարելու պետությունները:



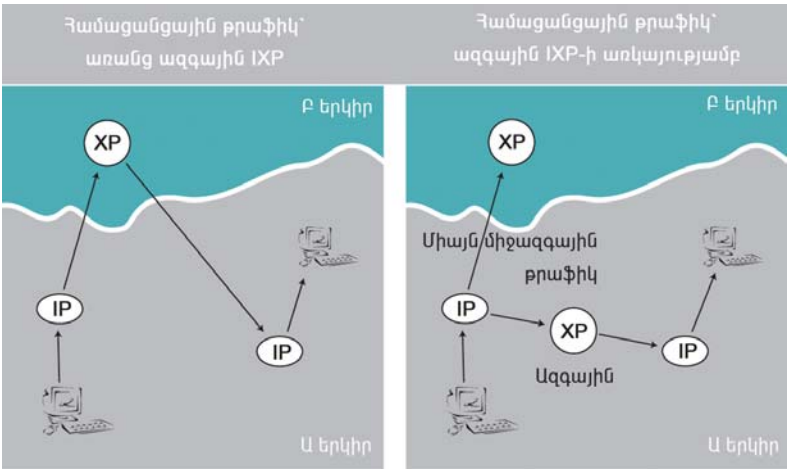
Երկրորդ՝ «ամպերում» պահվող անձնական տվյալների քանակի ավելացման հետ առաջին պլան կմղվեն տվյալների գաղտնիության և պահպանման հարցերը: Մենք, արդյոք, կվերահսկենք մեր տեքստային փաստաթղթերը (ֆայլերը), էլեկտրոնային փոստն ու այլ տվյալները: Օպերատորներն, արդյոք, կկարողանան դրանք օգտագործել առանց մեր թույլտվության: Ո՞վ է թույլտվություն ստանալու մեր տվյալները ձեռք բերելու:
Երրորդ՝ քաղաքացիների մասին տվյալների անընդհատ աճող ծավալի թվայնացման համապատասխան, պետություններին ավելի է անհանգստացնելու այն, որ իրենց ռեսուրսները գտնվում են «ազգային սահմաններից» դուրս: Հնարավոր է, որ նրանք փորձեն ստեղծել ազգային կամ տարածաշրջանային «ամպեր» կամ ապահովել գոյություն ունեցող «ամպերի» միջպետական վերահսկողության որոշակի աստիճան: «Ամպերի» ազգայնացման միտումը կարող է նաև ուժեղանալ այն պատճառով, որ այդ ճյուղի հիմնական օպերատորները հիմնավորված են ԱՄՆ-ում: Որոշ մարդիկ պնդում են, որ ICANN-ի շուրջ ընթացող վեճերը իրենց տեղը կարող են զիջել «տվյալների ամպային մշակումը» կարգավորելու մասին վեճերին:
Չորրորդ՝ քանի որ «տվյալների ամպային մշակման» ծառայությունները տարբեր օպերատորներ են տրամադրում, այդ պատճառով աճում է ստանդարտացման հարցերի նշանակությունը: Ընդհանուր ստանդարտների ընդունումը կապահովի տարբեր «ամպերի» միջև տվյալների անխափան փոխանցումը (օրինակ՝ Google-ի և Apple-ի միջև): Քննարկվում է բաց ստանդարտների ընդունման հնարավորությունը «տվյալների ամպային մշակման» շուկայում խաղի հիմնական մասնակիցների կողմից: Երբ խոսքն սկսում է վերաբերել այդ ոլորտին, հարցերն ավելի շատ են լինում, քան պատասխանները: Դրա կարգավորումը, հավանաբար, տարբեր ոլորտների մասնակիցների համագործակցության արդյունքն է լինելու: Օրինակ՝ Եվրամիությանն անհանգստացնում են տվյալների գաղտնիության և պահպանման հարցերը: «Անվտանգ նավահանգստի» մասին (Safe Harbour) համաձայնագիրը, որը մշակվել էր նպատակ ունենալով անձնական տեղեկատվության պահպանության տարբեր ռեժիմները համաձայնեցնելու ԱՄՆ-ում և ԵՄ-ում, անարդյունավետ էր: Համաձայն այն բանի, թե որքան շատ թվային տվյալներ են հատում Ատլանտյան օվկիանոսը, ԵՄ-ն ու ԱՄՆ-ն ստիպված են լինելու լուծել գաղտնիության ապահովման հարցերը՝ ամերիկյան ընկերությունների՝ «տվյալների ամպային մշակման» ոլորտում հիմնական օպերատորների կողմից ԵՄ ստանդարտների ընդունման հիման վրա: Ստանդարտացման ճյուղում խոշոր ընկերությունները, հավանաբար, կպայմանավորվեն: Google-ն արդեն ուժեղ մրցապայքար է սկսել՝ բաց ստանդարտների միավորման համար, ստեղծելով «տվյալների ազատագրման ճակատ», որի խնդիրն է ապահովել տարբեր «ամպերի» միջև տվյալների անխափան փոխանցումը: Դա համացանցում «տվյալների ամպային մշակումը» կարգավորելու համակարգի հիմքում դրված ընդամենն առաջին աղյուսներն են: Հավանաբար ի հայտ կգան հստակ քաղաքական հիմնախնդիրների նաև այլ լուծումներ:

Զուգամերձություն. համացանց-հեռահաղորդակցություն-բազմաֆունկցիոնալ մեդիա

Համացանցային արձանագրությունների լայնընդգրկուն և անընդհատ աճող օգտագործումը հանգեցրել է հեռահաղորդակցությունների, հեռուստա և ռադիոհաղորդումների, ինչպես նաև տեղեկատվության փոխանցման համակարգերի մերձեցման: Այսօր համացանցի օգնությամբ կարելի է հեռախոսազանգեր կատարել, ռադիո լսել, հեռուստածրագրեր դիտել և երաժշտություն փոխանակել: Ընդամենը մի քանի տարի առաջ այս խնդիրները կատարում էին տարբեր համակարգեր: Ավանդական հեռահաղորդակցությունների ոլորտում զուգամերձեցման հիմնական ուղղությունը համացանցային հեռախոսավարումն է (VoIP): Համացանցային հեռախոսավարման ծրագրերի աճող համբավը, ինչպիսին է, օրինակ՝ Skype-ը, հիմնված է ցածր գնային արժեքի, ձայնային շփման և տվյալների փոխանցման ուղիների միավորման, ինչպես նաև համակարգչային տարբեր գործիքների կիրառման հնարավորության վրա: YouTube-ի և նմանատիպ ցանցերի շնորհիվ, համացանցը միանում է նաև ավանդական մեդիա և զվարճալի ծառայություններին:

Մերձեցման գործընթացը տեխնիկական տեսանկյունից թեև շատ արագ է կատարվում, դրա տնտեսական և իրավական հետևանքներն ի հայտ են գալիս որոշ ժամանակ անց: Տնտեսական տեսանկյունից, տեխնոլոգիաների զուգամերձությունը սկսել է վերափոխել ավանդական շուկաները՝ նախկինում տարբեր ոլորտներում գործող ընկերություններին դարձնելով անմիջական մրցակիցներ: Այսպիսի պայմաններում ընկերություններն օգտագործում են տարբեր ռազմավարություններ, որոնցից ամենատարածվածը ձուլումն ու կլանումն է: Օրինակ՝ America Online (AOL) և Time Warner ընկերությունների միաձուլման նպատակը հեռահաղորդակցային ծառայությունների միավորումն էր մեդիա՝ զվարճալի ծառայությունների հետ: Ներկայում AOL/Time Warner-ը մեկ միասնական ընկերության ներքո միավորում է համացանցային պրովայդերների, հեռուստատեսությունը, երաժշտություն և կատարելագործում ծրագրային ապահովումը:

Իրավական համակարգն ավելի դանդաղ է ենթարկվում տեխնոլոգիաների մերձեցման հետ կապված փոփոխություններին: Հեռահաղորդակցության, հեռուստա և ռադիոհաղորդման, ՏՀՏ-ի յուրաքանչյուր հատվածն ունի սեփական չափորոշիչ բազա: Այդ ոլորտների միաձուլումը առաջ է քաշում մի շարք հարցեր, որոնք վերաբերում են կառավարմանն ու կարգավորմանը՝ ինչ տեղի կունենա գոյություն ունեցող ազգային և միջազգային կարգերի հետ այնպիսի ոլորտներում, ինչպիսիք են հեռախոսակապը կամ հեռուստառադիոհաղորդումները: Կմշակվե՞ն, արդյոք, առավելապես համացանցի հետ կապված նոր կարգեր: Զուգամերձության գործընթացի կարգավորումն, արդյոք, պետք է իրականացնեն պետական մարմինները (պետությունների կառավարությունները և միջազգային կազմակերպությունները), թե՞ ինքնակարգավորման մեթոդներով է իրականացվելու: Որոշ երկրներ, օրինակ՝ Մալազիան և Շվեյցարիան, ինչպես



նաև Եվրամիությունն արդեն այդ հարցերին իրենց պատասխաններն են առաջարկում: 1998 թ. Մալազիայում ընդունվեց բազմագործառութային մեդիայի և հեռահաղորդակցությունների մասին փաստաթուղթ, որը դրեց զուգամերձության գործընթացի կարգավորման համար ընդհանուր շրջանակների հիմքը: ԵՄ նոր շրջանակի հրահանգները, որոնք այսօր բարեփոխվել են ազգային օրենսդրության, համարվում են այդ ուղղությամբ արված այնպիսի մի քայլ, ինչպիսիք են Շվեյցարիայում գոյություն ունեցող հեռահաղորդակցությունների ոլորտի օրենքներն ու կանոնները: Շատ երկրներում համացանցի լայնագիծ ներթափանցումը մալուխային ցանցի միջոցով: Այն առավել ակտիվորեն է տեղի ունենում ԱՄՆ-ում, որտեղ մալուխային համացանցն ավելի տարածված է, քան ADSL-ը՝ լայնագիծ համացանցի երկրորդ հավանական տարբերակը: Գործառույթների այդպիսի միավորման հետ ինչ ռիսկեր են կապված: Բանավեճերի որոշ մասնակիցներ պնդում են, որ մալուխային ցանցերի օպերատորների դիրքը՝ որպես համացանցի և օգտատերերի միջև «թափարգելների» (բուֆերների), կարող է վտանգ ներկայացնել ցանցային չեզոքության սկզբունքի համար: ADSL տեխնոլոգիայով համացանց ավանդական ներթափանցման և մալուխային ցանցերի օգտագործման միջոցով ներթափանցման միջև եղած հիմնական տարբերությունն այն է, որ «մալուխը» չի ենթարկվում կապի, այսպես կոչված, բոլորին հասանելի ուղիների համար սահմանված գործողության կանոններին: Այդ կանոնները, որ կիրառվում են հեռախոսակապի համակարգի նկատմամբ, ներթափանցման տրամադրման գործում արգելում են որևէ խտրականություն: Մալուխային ցանցերի օպերատորների գործունեությունը չի կանոնակարգվում այդ կանոններով, ինչը նրանց հնարավորություն է տալիս լիարժեքորեն վերահսկելու իրենց հաճախորդների ներթափանցումը համացանց: Նրանք կարող են ուղեփակել որոշ հավելվածների օգտագործումը կամ կարգավորել որոշակի նյութերի ներթափանցումը: Օգտատերերին լրտեսելու և, որպես հետևանք, անձնական կյանքի գաղտնիք ունենալու նրանց իրավունքները խախտելու հնարավորությունը նույնպես էականորեն բարձր

է մալուխային համացանցում, քանի որ ներթափանցումն իրականացվում է տեղային ցանցերին համապատասխան համակարգերի օգնությամբ: Այդ թեմայի վերաբերյալ Քաղաքացիական ազատությունների համար ամերիկյան միության հրապարակած զեկուցման մեջ բերվում է մալուխային համացանցի մենաշնորհման առնչությամբ ռիսկերի հետևյալ օրինակը. «Դա նույնն է, թե հեռախոսային ընկերությանը թույլատրեն որպես սեփականություն ունենալ ռեստորաններ և «Domino's» ռեստորան զանգող հաճախորդներին տրամադրել որակյալ ծառայություններ ու անխափան կապ, իսկ «Pizza Hut» զանգահարողներին մշտապես տալ «զբաղված է» ազդանշանը, կապի խզում և խափանումներ»:

Այս հիմախնդիրը կարող է լուծվել այն ժամանակ, երբ մշակվի հստակ սահմանում այն մասին, թե ինչ է մալուխային համացանցը՝ «տեղեկատվական ծառայություն» թե «հեռահաղորդակցային ծառայություն»: Եթե երկրորդ տարբերակն ընտրվի, ապա մալուխային համացանցը կկարգավորվի բոլորին հասանելի կապուղիների համար սահմանված կանոններով:

Կիբեռանվտանգություն

Արդի վիճակ

Համացանցն ի սկզբանե ստեղծվել էր սահմանափակ շրջանակի անձանց օգտագործման համար, այդ պատճառով անվտանգության հարցերին, եթե, իհարկե, դրանք երբևէ ուշադրության են արժանացել, նշանակություն չի տրվել: Ակադեմիական միության անդամները, ովքեր համացանցի հիմնական օգտատերերն էին, մշակել են ազդեցիկ, էական կանոններ՝ նպատակ ունենալով ապահովել համացանցի անվտանգությունը: Կիբեռանվտանգության հարցերը հրատապ դարձան համացանցի օգտատերերի քանակի կտրուկ աճի հետևանքով: Համացանցը հաստատեց այն երկյուղը, որը վաղուց շատերն ունեին՝ տեխնոլոգիան կարող է միաժամանակ նոր հնարավորություններ տրամադրել և վտանգներ հարուցել:

Այն ամենը, որ կարող է օգտագործվել հասարակության բարօրության համար, կարող է նաև օգտագործվել ի վնաս նրա: Մարդու գործունեության համարյա բոլոր բնագավառներում համացանցի արագընթաց ներմուծման վնասակար հետևանքը համարվում է ժամանակակից հասարակության բարձր խոցելիությունը: Համացանցը դարձել է գլոբալ վտանգավոր ենթակառուցվածքի մի մասը, այնպիսի բաղադրիչների շարքում է, ինչպիսիք են՝ էլեկտրական ցանցերը, տրանսպորտային և առողջապահության համակարգերը: Քանի որ այդ համակարգերի դեմ հարձակումները կարող են դրանց գործառույթների լուրջ խախտումներ և լուրջ ֆինանսական հետևանքներ առաջ բերել, ենթակառուցվածքի խիստ կարևոր տարրերը շատ հաճախ են դառնում հարձակումների օբյեկտ: Կիբեռանվտանգության հարցերը կարելի է դասակարգել երեք չափանիշի՝ գործողության տեսակ,

հանցագործի տեսակ և նպատակի տեսակ: Գործողությունների տեսակի վրա հիմնված դասակարգումը կարող է ներառել՝ տվյալների բռնագրավում, տվյալների ամբողջականության խախտում, արգելված ներթափանցում, լրտեսական ծրագրերի ապահովման ներդրում, տվյալների փոփոխում, տեղեկատվական դիվերսիա, ծառայությունների նորմալ տրամադրման խախտում (DoS-հարձակում) և անձի առևանգում:
Հավանական հանցագործների տեսակներն են՝ հակերները, կիբեռհանցագործները, կիբեռռազմիկները և կիբեռահաբեկիչները:
Ենթադրյալ նպատակները բազմաթիվ են՝ անհատից, մասնավոր ընկերություններից և պետական հիմնարկություններից մինչև վտանգավոր ենթակառուցվածքները, կառավարությունները և զինվորական օբյեկտները:

Մանրամասն կիբեռանվտանգության վերաբերյալ բաժին 3-ում

Կիբեռանվտանգության բնագավառում քաղաքական նախաձեռնությունները

Կիբեռանվտանգության հարցերին են նվիրված շատ ազգային, տարածաշրջանային և գլոբալ նախաձեռնություններ: Ազգային մակարդակում կիբեռանվտանգության ճյուղում ավելանում է օրենսդրական փաստաթղթերի և դատական գործերի թիվը: Առավել հայտնի են ԱՄՆ նախաձեռնությունները՝ ահաբեկչության դեմ պայքարում պետության լիազորություններն ընդլայնելու առնչությամբ: Համացանցի անվտանգության հարցերով զբաղվող հիմնական գերատեսչությունը ԱՄՆ ներքին անվտանգության նախարարությունն է: Դժվար է գտնել մի զարգացած երկիր, որտեղ կիբեռանվտանգությանն առնչվող որևէ նախաձեռնություն չլինի: Միջազգային մակարդակով ամենաակտիվ կազմակերպությունը ՀՄՄ-ն է, որը մշակել է անվտանգության բազմաբանակ շրջանակաձև փաստաթղթեր, կառույցներ և ստանդարտներ՝ ներառյալ X.509-ը: Այդ ստանդարտը «բաց բանալի» (PKI) ենթակառուցվածքի հիմքն է, որն օգտագործվում է, օրինակ՝ HTTP (HTTPS) արձանագրության պաշտպանված մեկնակերպում (վերսիայում): Բոլորովին վերջերս ՀՄՄ-ն, զուտ տեխնոլոգիական տեսանկետների շրջանակից դուրս եկավ և գործի դրեց «Կիբեռանվտանգության բնագավառում ՀՄՄ-ի գլոբալ օրակարգը»[35] նախաձեռնությունը: Այդ նախաձեռնությունը նախատեսում է իրավական միջոցառումներ, քաղաքական համագործակցություն և օգնություն զարգացող երկրներին: Կիբեռանվտանգության բնագավառում «Մեծ ութնյակը» նույնպես հանդես եկավ մի քանի նախաձեռնություններով, որոնք ուղղված էին իրավապահ մարմինների համագործակցության մեխանիզմների կատարելագործմանը: Այդ կազմակերպությունն ստեղծել է բարձր տեխնոլոգիաների ոլորտում հանցագործությունների գծով ենթախումբ՝ մասնակից պետությունների կիբեռանվտանգության կենտրոնների միջև մշտական (օրվա 24 ժամը և

շաբաթվա 7 օրը) հեռահաղորդակցային կապ հաստատելու, անձնակազմի նախապատրաստման և պետությունների իրավական համակարգերի կատարելագործման համար: Ենթախումբը կոչված է հակազդելու կիբեռհանցագործությանը և նպաստելու ՏՀՏ արդյունաբերության ու իրավապահ մարմինների միջև համագործակցության զարգացմանը: ՄԱԿ-ի Գլխավոր գագաթաժողովը վերջին մի քանի տարվա ընթացքում մի շարք բանաձևեր է ընդունել «միջազգային անվտանգության համատեքստում տեղեկատվական և հեռահաղորդակցությունների բնագավառում նվաճումների» վերաբերյալ, մասնավորապես, 53/70 (1998), 54/49 (1999), 55/28 (2000), 56/19 (2001), 57/239 (2002) и 58/199 (2003) բանաձևերը: 1998 թ.-ից սկսած հաջորդող բոլոր բանաձևերը միանման բովանդակություն ունեն՝ առանց էական բարելավումների: Դրանք չեն արտացոլում 1998 թ.-ից սկսած կիբեռանվտանգության ոլորտում տեղի ունեցած նշանակալի փոփոխությունները: Համացանցի անվտանգությանն առնչվող միջազգային իրավական կարևորագույն գործիք է 2004 թ. հուլիսի 1-ին ուժի մեջ մտած կիբեռհանցագործության վերաբերյալ ԵԽ համաձայնագիրը[36]: Որոշ երկրներ կնքել են նաև երկկողմանի պայմանագրեր: Քրեական հանցագործությունների հարցերով իրավական համագործակցության մասին ԱՄՆ-ն երկկողմանի պայմանագրեր է կնքել ավելի քան 20 երկրների հետ[37]: Այդ պայմանագրերը կիրառելի են նաև կիբեռհանցագործությունների դեպքում:

Հետազոտողների և ոչ կառավարական կազմակերպությունների ուժերով այս ոլորտում միջազգային պայմանագիր մշակելու փորձերից մեկը կիբեռհանցագործություններից և կիբեռահաբեկչությունից պաշտպանելու մասին Սթենդֆորդի նախնական համաձայնագիրն է: Այդ փաստաթուղթը խորհուրդ է տալիս ստեղծել միջազգային մարմին, որը կոռվելու է՝ Տեղեկատվական ենթակառուցվածքի պաշտպանության գործակալություն:

Հարցեր

Համացանցի կառուցվածքի ազդեցությունը կիբեռանվտանգության վրա

Համացանցի անվտանգության վրա ազդում են իր իսկ կառուցվածքի առանձնահատկությունները: Մենք, արդյոք, պե՞տք է շարունակենք կառչել ներկա մոտեցմանը՝ փորձելով վերևում գոյություն ունեցող վտանգավոր հիմքի վրա անվտանգություն «կառուցել», թե՞ հարկ է ինչ-որ բան փոխել համացանցի ենթակառուցվածքի հիմքում: Այդպիսի փոփոխություններն ինչպե՞ս կազդեն համացանցի մյուս հատկանիշների վրա, մասնավորապես, դրա թափանցիկության և բաց լինելու հատկության վրա: Համացանցի ստանդարտների մշակման ուղղությամբ նախկին նախաձեռնությունների մեծ մասը հետապնդում էր նոր հավելվածների արդյունավետության կամ ներդրման բարելավման նպատակ: Անվտանգությունը գերակայություն չէր: Հնարավոր չէ կանխատեսել, արդյոք IETF-ն կարո՞ղ է փոխել էլեկտրոնային փոստի ստանդարտները, որպեսզի երաշխավորի

իսկության հավաստիությունը (աուտենտիֆիկացիա) և արդյունքում կրճատի համացանցի անպատշաճ օգտագործումը (օրինակ՝ սպամը, կիբեռանվտանգությունը): Հաշվի առնելով համացանցի հիմնական ստանդարտների ամեն մի փոփոխության հետ կապված հակասությունները, հավանական է, որ համացանցի բազային հավելվածների կատարելագործումն անվտանգության ոլորտում դանդաղ և աստիճանաբար է ընթանալու:

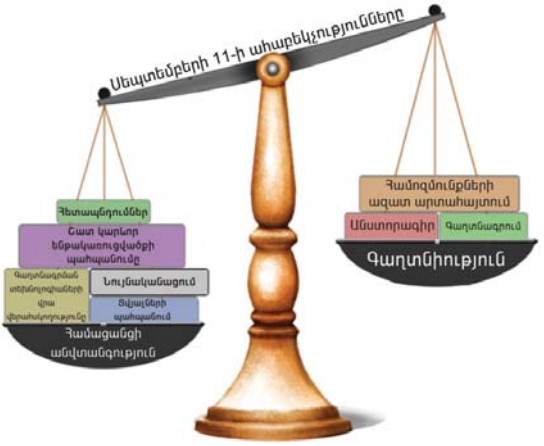
Էլեկտրոնային առևտրի հետագա զարգացումը պահանջում է կիբեռանվտանգության բարձր մակարդակ

Կիբեռանվտանգության մասին ավելի հաճախ հիշատակում են էլեկտրոնային առևտրի արագ զարգացման համար նախնական պայմանների շարքում: Քանի դեռ համացանցը պաշտպանված ու հուսալի չէ, հաճախորդները համացանցի միջոցով գաղտնի տեղեկատվությունը դժկամորեն կտրամադրեն (օրինակ՝ վարկային քարտերի համարները): Նույնը վերաբերում է նաև համացանցում բանկային ծառայություններին և էլեկտրոնային փողերի օգտագործմանը: Եթե կիբեռանվտանգության ընդհանուր մակարդակի բարձրացումը դանդաղ ընթանա (օրինակ՝ ստանդարտների բացակայության պատճառով), հավանական է, որ գործարար կառույցները կնպաստեն կիբեռանվտանգության արագ զարգացմանը: Այդպիսի պայմաններում ցանցային չեզոքության սկզբունքի համար նոր վտանգներ կարող են ծագել, ինչպես նաև «նոր համացանց» ստեղծելու նախադրյալներ կստեղծվեն, որն, ամեն ինչից զատ, կօգնի համացանցում հեռահաղորդակցությունն ավելի անվտանգ դարձնել:

Կիբեռանվտանգությունն ու մասնավոր կյանքի գաղտնիքը

Վիճելի հարցերից մեկը մասնավոր կյանքի անվտանգության և գաղտնիության պահպանման միջև փոխադարձ կապն է: Կիբեռանվտանգության ապահովումն, արդյոք, կպահանջի այնպիսի միջոցներ ձեռնարկել, որոնք ենթադրում են մասնավոր կյանքի գաղտնիության իրավունքից մասնակի հրաժարում: Գաղտնագրման համար ծրագրային ապահովման կիրառումն ինչպե՞ս պետք է կարգավորվի, որ կարողանա օգտագործվել և նամակագրության գաղտնիության օրինական պահպանման համար, և ահաբեկիչների ու հանցագործների անօրինական հեռահաղորդակցությունների պահպանման համար: Այս և այլ հարցերի պատասխանը կախված է կիբեռանվտանգության և մասնավոր կյանքի անձեռնմխելիության միջև անընդհատ տատանվող հավասարակշռությունից: 2001 թ. սեպտեմբերի 11-ին Նյու Յորքում տեղի ունեցած ահաբեկչությունից հետո ԱՄՆ-ում անվտանգության նկատառումներն առաջին տեղում դրվեցին, որի արդյունքը համացանցում ավելի ակտիվ լրտեսում նախատեսող մի շարք օրենսդրական փաստաթղթերի ընդունումն էր: Քաղաքացիական հասարակության ներկայացուցիչները դրան արձագանքեցին՝ ուշադրություն հրավիրելով մասնավոր կյանքի գաղտնիքների պաշտպանության

Ենթակառուցվածք և ստանդարտացում



և համոզմունքների ազատ արտահայտման սկզբունքներին: ՏՀՏ անվտանգության ապահովման և մասնավոր կյանքի գաղտնիքի պահպանման միջև միջազգային մակարդակով հավասարակշռության հարցը գտնվում էր կիբեռանվտանգության վերաբերյալ Եվրոպայի խորհրդի պայմանագիրը գլոբալ մակարդակով տարածման մասին քննարկումների կենտրոնում: Մարդու իրավունքները պաշտպանող ակտիվիստների հիմնական առարկությունն այն էր, որ պայմանագիրը ձգտում է կիբեռանվտանգության հիմնախնդիրները լուծել մասնավոր կյանքի գաղտնիքների և մարդու մյուս իրավունքների հաշվին:

Գաղտնագրում

Համացանցի անվտանգության ապահովման վերաբերյալ քննարկումների կարևորագույն հարցերից է գաղտնագրման հիմնախնդիրը կամ գաղտնագրային պահպանությունը, որը վերաբերում է փոխանցվող տվյալների պաշտպանության համար օգտագործվող գործիքներին: Մաթեմատիկական որոշակի ալգորիթմների օգնությամբ գաղտնագրման ծրագրային ապահովումը (ԾԱ) էլեկտրոնային հեռահաղորդակցությունը (էլեկտրոնային փոստը, պատկերները) կողմնակի անձանց համար անհասկանալի է դարձնում: Որոշակի տեղեկատվության գաղտնիությունն ապահովելու անհրաժեշտության և հավանական հանցագործ կամ ահաբեկչական գործունեությանը հետամուտ լինելու կառավարությունների պահանջների միջև հավասարակշռությունն այդպես էլ չի գտնվել: Գաղտնագրման պաշտպանության առնչությամբ վարվող քաղաքականության միջազգային տեսակետները վերաբերում են համացանցի կառավարման ոլորտին, քանի որ գաղտնագրման կարգավորումը պետք է լինի գլոբալ կամ, ծայրահեղ դեպքում, վերաբերի բոլոր այն երկրներին, որոնք ընդունակ են արտադրելու

Մանրամասն խոսքի ազատության վերաբերյալ բաժին 6-ում

գաղտնագրման գործիքներ: Օրինակ՝ գաղտնագրման համար ԾԱ արտահանումը վերահսկելու ուղղությամբ ԱՄՆ քաղաքականությունն այնքան էլ հաջողված չէր, քանի որ ԱՄՆ-ն չէր կարող վերահսկել միջազգային մակարդակով այդպիսի ԾԱ-ի տարածումը: ԾԱ արտադրող ամերիկյան ընկերությունները սկսել են հզոր լոբբիստական մրցապայքար, որի հիմնական գաղափարն այն էր, որ արտահանման վերահսկումը ոչ թե ամրապնդում է ազգային անվտանգությունը, այլ միայն խախտում է ամերիկյան բիզնեսի դիրքերը:

Գաղտնագրման գործիքներին վերաբերող միջազգային կարգերը

Տեղեկատվության գաղտնագրային պաշտպանության հարցերը մինչ օրս դիտարկվել են երկու համատեքստում՝ Վասենարյան պայմանագրի և Տնտեսական համագործակցության ու զարգացման կազմակերպության (ՏՀՁԿ, Organization for Economic Co-operation and Development, OECD): Վասենարյան պայմանագիրը 33 զարգացած երկրների հաստատած միջազգային կարգ է[2], որի նպատակն է սովորական սպառազինության և «երկակի նշանակության» տեխնոլոգիաների արտահանման սահմանափակումը դեպի պատերազմող երկրներ և «անջատվող երկրներ»: Պայմանագրի համաձայն, Վիեննայում ստեղծվել է քարտուղարություն: Վասենարյան պայմանագրի շրջանակներում ԱՄՆ լոբբիստական ջանքերի նպատակն էր միջազգային մակարդակով տարածել «Կլիպեր չիպ» 3 տեխնոլոգիայի սկզբունքով մոտեցումը, որը թույլ էր տալիս վերահսկել ծածկագրման ԾԱ-ը՝ բանալիների ավանդադրման համակարգի օգնությամբ: Դրան հակադրվեցին շատ երկրներ, հատկապես Ճապոնիան և Սկանդինավյան պետությունները: 1998 թ. փոխզիջման հասան՝ շնորհիվ գաղտնագրման չափանիշների ներդրման, որոնց համաձայն, ծածկագրման սարքերի վերահսկման ցուցակում և «երկակի նշանակության» ԾԱ մեջ ընդգրկվել են բանալիի 56 բիտ և ավելի երկարությամբ արտադրանքներ: Այս կարգը վերաբերում էր նաև այնպիսի համացանցային ծրագրերի, ինչպիսիք են՝ բրաուզերները և էլեկտրոնային փոստի հաճախորդները: Հետաքրքիր է այն, որ այդ պայմանագիրը չի շոշափում տեխնոլոգիաների փոխանցման «աննշան» տեսակները (օրինակ՝ համացանցում նշոցի (ֆայլի) բեռնումը): «Կլիպեր չիպ» միջազգային մեկնակերպի ներմուծման անհաջողությունը նպաստեց, որ ԱՄՆ կառավարությունը դադարեց առաջ քաշել այդ տեխնոլոգիան նաև իր երկրի ներսում: Այդ օրինակը ցույց է տալիս ազգային և միջազգային ասպարեզում տեղի ունեցող իրադարձությունների կապը. այս դեպքում միջազգային իրադարձությունները վճռական ազդեցություն ունեին ազգայինների վրա: ՏՀՁԿ- ն տվյալների գաղտնագրման բնագավառում միջազգային համագործակցության ևս մեկ հարթակ է: ՏՀՁԿ-ի փաստաթղթերը թեև պարտադիր իրավական ուժ չունեն, սակայն տարբեր հարցերի վերաբերյալ դրա հրահանգները մեծ հեղինակավոր են համարվում: Դրանք ի հայտ են գալիս փորձագետների աշխատանքի և համաձայնության հիման վրա ընդունված որոշումների արդյունքում: Այդպիսի հրահանգների

մեծ մասն ընդգրկվում է ազգային օրենքների մեջ: Գաղտնագրման պաշտպանության ոլորտում ՏՀԶԿ-ի գործունեությունը շատ վեճեր էր հարուցում: Դրա սկիզբը դրվել է 1996 թ., երբ ԱՄՆ-ն առաջարկեց ընդունել բանալիների ավանդադրման համակարգը՝ որպես միջազգային ստանդարտ: Ինչպես Վասենարյան պայմանագրի դեպքում, ԱՄՆ առաջարկի վերաբերյալ բանակցությունները ևս Ճապոնիայի և սկանդինավյան պետությունների ուժեղ հակազդեցությունն առաջացրին: Արդյունքում ի հայտ եկավ գաղտնագրման պաշտպանության ոլորտի քաղաքականության հիմնական բաղադրիչների համաձայնեցման մեկնակերպը:

2. 2010 թ. սկզբին պայմանագրին մասնակից էր 40 պետություն:
3. Հեռախոսային խոսակցությունների գաղտնագրային պաշտպանության ապահովման համակարգը, որը 1993 թ. առաջարկել էր ԱՄՆ իշխանությունը: Դրա համաձայն, խոսակցությունների գաղտնագրումը կարող է իրականացվել միայն տեխնիկական միջոցների օգնությամբ, որոնք անհրաժեշտության դեպքում իրավապահ մարմինները կարող են գաղտնազերծել՝ նախօրոք «երրորդ կողմից» որպես ավանդ վերցված թույլտվության հատուկ բանալու օգնությամբ: Այդ նախագծին կտրուկ ընդդիմացավ ամերիկյան հասարակությունը և այն այդպես էլ չիրականացվեց:

Գաղտնագրման միջազգային կարգ ստեղծելու մի քանի փորձերն առավելապես Վասենարյան պայմանագրի համատեքստում, չհանգեցրին միջազգային գործուն կարգի հաստատման: Մինչ օրս համացանցում կարելի է ձեռք բերել գաղտնագրման պահպանության հզոր գործիքներ:

Փոստաղբ

Արդի վիճակ

Փոստաղբը սահմանվում է որպես փոստ ստացողի չպահանջված էլեկտրոնային նամակագրություն, որն առաքվում է համացանցի մեծ թվով օգտատերերի: Փոստաղբը հիմնականում օգտագործվում է գովազդի նպատակով: Այս ամենի հետ, փոստաղբն առաքվում է հասարակական մրցապայքար, քաղաքական քարոզչություն վարելու և պոռնոգրաֆիական նյութեր տարածելու համար: Փոստաղբի հիմնախնդիրը ընդգրկված է ենթակառուցվածքին հատկացված «արկղի» մեջ, քանի որ այն խոչընդոտում է համացանցի նորմալ գործառույթներին՝ խանգարելով համացանցային հիմնական հավելվածներից մեկի՝ էլեկտրոնային փոստի աշխատանքին: Սա համացանցի կառավարման հիմնախնդիրներից մեկն է, որ վերաբերում է յուրաքանչյուր օգտատիրոջ: Վերջին վիճակագրության համաձայն, էլեկտրոնային 20 հաղորդագրություններից 19 կարելի է որակավորել որպես փոստաղբ: Բացի այն բանից, որ փոստաղբը

դժգոհություն է առաջացնում, այն նաև անցաթղթային ունակության ծախսերի և ժամանակի առումով հանգեցնում է էական տնտեսական կորստի, որը վատնվում է փոստաղբը կարդալու և ջնջելու համար: Վերջին ժամանակների որոշ ուսումնասիրություններ ցույց են տվել, որ փոստաղբի հետ կապված միայն անցաթղթային ունակության կորուստը կազմում է տարեկան մոտավորապես 10 մլրդ եվրո: Փոստաղբի դեմ կարելի է պայքարել ինչպես տեխնիկական, այնպես էլ իրավաբանական միջոցներով: Տեխնիկական տեսակետից հաղորդագրությունները զտող և փոստաղբը հեռացնող շատ ծրագրեր գոյություն ունեն: Զտման համակարգերի հիմնական բարդությունն այն է, որ դրանք երբեմն հեռացնում են այնպիսի հաղորդագրություններ, որոնք փոստաղբ չեն: Փոստաղբին հակազդող արդյունաբերությունը զարգացող հատված է, որտեղ մշակվում են փոստաղբը սովորական նամակագրությունից զանազանելու ավելի բարդ մեխանիզմներ: Սակայն տեխնիկական մեթոդները միայն սահմանափակ ազդեցություն ունեն, և դրանց կիրառումն անհրաժեշտ է ուղեկցել ստույգ իրավական միջոցներով: Ինչ վերաբերում է հարցի իրավական տեսանկյունին, նշենք, որ շատ երկրներում փոստաղբի դեմ պայքարի օրենսդրություն է ընդունվել: ԱՄՆ-ում փոստաղբի և գովազդի համար էլեկտրոնային փոստի օրինական կիրառման միջև ճկուն սահման գտնելու փորձը ձեռնարկվել է, այսպես կոչված, Can-Spam Act-ում38: Օրենքը, թեև խիստ պատիժ է նախատեսում փոստաղբի տարածման համար, ընդհուպ հինգ տարվա ազատազրկում, սակայն օրենքի քննադատները պնդում են, որ դրա որոշ դրույթներ փոստաղբի հանդեպ հանդուրժող են ու նույնիսկ կարող են նպաստել դրա տարածմանը: Օրենքում նշված սկզբնական դիրքորոշման համաձայն, նախատեսվում է, որ փոստաղբը թույլատրվում է այնքան ժամանակ, քանի դեռ այդպիսի հաղորդագրություններ ստացողը չի պահանջում դադարեցնել դրանք (օգտագործելով առաքումներից հրաժարվելու իր իրավունքը): 2003 թ. դեկտեմբերից սկսած, երբ օրենքն ընդունվեց, վիճակագրությունը փոստաղբի քանակի կրճատում չի գրանցել: 2003 թ. հուլիսին Եվրամիությունում ընդունվեց փոստաղբի դեմ պայքարի սեփական օրենքը, որը դարձավ գաղտնիության և էլեկտրոնային հեռահաղորդակցությունների մասին հրահանգի մի մասը: ԵՄ օրենսդրությունը շեշտադրում է փոստաղբի կրճատմանը նպաստող մասնավոր սեկտորի ինքնակարգավորումն ու նախաձեռնողականությունը[39]: 2006 թ. նոյեմբերին Եվրահանձնաժողովը հաղորդագրություն է թողարկում փոստաղբի, լրտեսական և հակաօրինական ԾԱ դեմ պայքարի մասին: Հաղորդագրության մեջ թվարկված են մի շարք գործողություններ, որոնք անհրաժեշտ են արդեն գոյություն ունեցող օրենսդրության կատարումն ապահովելու համար, քանի որ, ըստ փաստաթղթի հեղինակների, հիմնական խնդիրը հենց դա է:

Փոստաղբն ու «նորաձևությունը քաղաքականության մեջ»

Փոստաղբը գլոբալ քաղաքականության մեջ միտումների, որոշ դեպքերում նաև «նորաձևության» փայլուն օրինակ է: 2005 թ. WGIG հաշվետվության մեջ որպես կարևոր ոլորտ նշված համացանցի կառավարման լուրջ հիմսախնդիր էր դարձել փոստաղբը: Այն քննարկվել էր WSIS թունիսյան փուլի, ինչպես նաև միջազգային մի շարք այլ հանդիպումների ընթացքում: Սպամի հիմսախնդիրը լայնորեն լուսաբանվում էր նաև մամուլում: Ամենահամեստ գնահատականների համաձայն, 2005 թ.-ից սկսած փոստաղբի ծավալը եռապատկվել է (2005 թ. մեկ օրում՝ 30 մլրդ հաղորդագրություն, 2008 թ. մեկ օրում՝ 100 մլրդ հաղորդագրություն): Սպամի քաղաքական նշանակությունը չի համապատասխանում վիճակագրությանը: Գլոբալ քաղաքականության մեջ փոստաղբի հիմսախնդիրը համարյա նկատելի չէ: Հայդարաբադում համացանցի կառավարման մասին համաժողովի ընթացքում փոստաղբը հիշատակվել է ընդամենը մեկ սեմինարի ժամանակ (առաջարկվել էր անցկացնել 91 սեմինար): Փոստաղբի հանդեպ համաշխարհայնացված (գլոբալ) քաղաքականության նմանատիպ փոփոխությունների պատճառները դեռևս պետք է պարզաբանվի:

Միջազգային նախաձեռնություններ

Փոստաղբին հակազդելու մասին օրենքները, որ ընդունվել են ինչպես ԱՄՆ-ում, այնպես էլ ԵՄ-ում, ունեն մի թույլ տեղ՝ անդրսահմանային փոստաղբի կանխարգելման միջոցների բացակայությունը: Այս հիմսախնդիրը հատկապես հրատապ է այնպիսի երկրների համար, ինչպիսին է Կանադան, որը վիճակագրության վերջին տվյալների համաձայն, փոստաղբ հաղորդագրությունների 20-ից 19 ստանում է արտասահմանից: Կանադայի արդյունաբերության նախարար Լյուսիեն Ռոբիյարը վերջերս հայտարարել է, որ այդ հիմսախնդիրը չի կարող լուծում գտնել «առանձին վերցրած երկրում»: Նմանատիպ եզրակացության էին եկել նաև փոստաղբի դեմ հակազդեցության մասին ԵՄ երկրների ընդունած օրենքների ուսումնասիրությունների հեղինակները: Այդ ուսումնասիրությունները վերջերս անցկացրել էր Ամստերդամի համալսարանի տեղեկատվական իրավունքի ինստիտուտը. «Այն փաստը, որ փոստաղբ-հաղորդագրությունների զգալի մասի աղբյուրները գտնվում են ԵՄ-ից դուրս, էականորեն սահմանափակում է ԵՄ հրահանգի արդյունավետությունը»: Հարկավոր է գտնել գլոբալ լուծում, որը հիմված լինի միջազգային պայմանագրի կամ համանման մի մեխանիզմի վրա: Ավստրալիայի, Կորեայի և Մեծ Բրիտանիայի համատեղ ստորագրած փոխըմբռնման հուշագիրը փոստաղբի դեմ պայքարի գործում

Փոստաղբն ու «նորաձևությունը քաղաքականության մեջ»

Փոստաղբը գլոբալ քաղաքականության մեջ միտումների, որոշ դեպքերում նաև «նորաձևության» փայլուն օրինակ է: 2005 թ. WGIG հաշվետվության մեջ որպես կարևոր ոլորտ նշված համացանցի կառավարման լուրջ հիմնախնդիր էր դարձել փոստաղբը: Այն քննարկվել էր WSIS թունիսյան փուլի, ինչպես նաև միջազգային մի շարք այլ հանդիպումների ընթացքում: Սպամի հիմնախնդիրը լայնորեն լուսաբանվում էր նաև մամուլում: Ամենահամեստ գնահատականների համաձայն, 2005 թ.-ից սկսած փոստաղբի ծավալը եռապատկվել է (2005 թ. մեկ օրում՝ 30 մլրդ հաղորդագրություն, 2008 թ. մեկ օրում՝ 100 մլրդ հաղորդագրություն): Սպամի քաղաքական նշանակությունը չի համապատասխանում վիճակագրությանը: Գլոբալ քաղաքականության մեջ փոստաղբի հիմնախնդիրը համարյա նկատելի չէ: Հայդարաբադում համացանցի կառավարման մասին համաժողովի ընթացքում փոստաղբը հիշատակվել է ընդամենը մեկ սեմինարի ժամանակ (առաջարկվել էր անցկացնել 91 սեմինար): Փոստաղբի հանդեպ համաշխարհայնացված (գլոբալ) քաղաքականության նմանատիպ փոփոխությունների պատճառները դեռևս պետք է պարզաբանվի:

միջազգային համագործակցության առաջին օրինակներից է: Տնտեսական համագործակցության և զարգացման կազմակերպությունում (ՏՀԶԿ) ստեղծվել է փոստաղբով զբաղվող աշխատանքային խումբ և պատրաստվել է փոստաղբի դեմ պայքարի «գործիքների հավաքածու»: ՀՄՄ-ն այդ հարցում նույնպես ակտիվ դիրք է գրավել՝ ստեղծելով փոստաղբի տարածման դեմ հակազդեցությունների հարցերի վերաբերյալ թեմատիկ խորհրդակցություն (2004), նպատակ ունենալով քննարկելու փոստաղբի դեմ հակազդեցության ոլորտում փոխըմբռնման մասին գլոբալ հուշագիր ստորագրելու տարբեր հնարավորությունները: ԵՄ-ում տարածաշրջանային մակարդակով ստեղծվել է փոստաղբի դեմ պայքարի միջոցների ներդրման գործակալությունների ցանց, իսկ Ասիա-խաղաղօվկիանոսյան տնտեսական համագործակցության (ԱխՏՀ) շրջանակներում կազմվել է «Օգտատիրոջ ուղեցույց»: Փոստաղբի դեմ պայքարի մեկ այլ հավանական մոտեցում են ցուցաբերում էլեկտրոնային փոստի ծառայություններ մատակարարող առաջադեմ համացանցային ընկերությունները, ինչպիսիք են՝ America Online, British Telecom, Comcast, EarthLink, Microsot и Yahoo!: Նրանք ստեղծել են Փոստաղբի դեմ հակազդեցության տեխնիկական միություն (ASTA), որի հիմնական խնդիրը սպամի դեմ պայքարի բնագավառում տեխնիկական ու քաղաքական նախաձեռնությունների համակարգումն է:

Հարցեր

Փոստաղբի տարբեր սահմանումները

Փոստաղբի վերաբերյալ տարբեր ընկալումներն ազդում են դրա դեմ պայքարի արդյունավետության վրա: ԱՄՆ-ում այդ պայքարին խանգարում է խոսքի ազատության պաշտպանության մասին և Սահմանադրությանը վերաբերող առաջին փոփոխության մտահոգությունը: Ամերիկացի օրենսդիրները փոստաղբ են համարում միայն «առևտրային այն հաղորդագրությունները, որոնք չի պահանջում օգտատերը», իսկ մյուս բոլոր տեսակի փոստաղբերն (քաղաքական քարոզչություն և

պոռնոգրական նյութեր) անուշադրության է մատնում: Երկրների մասում դոստաղը է համարվում «էլեկտրոնային զանգվածային այն առաքում-հաղորդագրությունները, որոնք օգտատերը չի պահանջում»՝ անկախ դրա բովանդակությունից: Քանի որ փոստաղբի հիմնական աղբյուրը ԱՄՆ-ն է, ապա սահմանումների այդպիսի տարընթերցումը իրականում սահմանափակում է փոստաղբի դեմ պայքարի միջազգային արդյունավետ մեխանիզմի ստեղծման ամեն մի հնարավորություն:

Փոստաղբն ու էլեկտրոնային հաղորդագրությունների իսկության վավերացումը

Փոստաղբի կառուցվածքային նախադրյալներից մեկը օգտատիրոջը կեղծ հասցեներով էլեկտրոնային հաղորդագրություններ ուղարկելու հնարավորությունն է: Այս հիմնախնդրի համար գոյություն ունի տեխնիկական լուծում, որի ներմուծումը պահանջում է ներկայում կիրառվող էլեկտրոնային փոստի ստանդարտների փոփոխություններ իրականացնել: Համացանցի նախագծման աշխատանքային խումբն ուսումնասիրում է էլեկտրոնային փոստի արձանագրությունների փոփոխությունների հնարավորությունը, որպեսզի երաշխավորի էլեկտրոնային հաղորդագրությունների իսկությունը: Սա այն օրինակներից մեկն է, թե ինչպես են տեխնիկական հարցերն (ստանդարտները) ազդում քաղաքականության վրա: Միակ հավանական զիջումը, որն անհրաժեշտ է կատարել էլեկտրոնային հաղորդագրությունների իսկությունն ապահովելու համար, համացանցում անստորագիր հաղորդագրությունների սահմանափակումն է:

Գլոբալ մակարդակով գործողությունների անհրաժեշտությունը

Վերը նշվեց, որ փոստաղբի մեծ մասը գալիս է արտասահմանից: Դա գլոբալ հիմնախնդիր է, որը պահանջում է գլոբալ լուծում: Գոյություն ունեն տարբեր նախաձեռնություններ, որոնք կարող են հանգեցնել գլոբալ համագործակցության արդյունավետության բարձրացման: Դրանցից մի քանիսն արդեն հիշատակվել են, օրինակ՝ փոխըմբռնման մասին երկկողմանի հուշագրերը: Մյուսները ներառում են, օրինակ՝ ներուժի հզորացումը և տեղեկատվության փոխանակումը: Առավել համապարփակ լուծում է պահանջում փոստաղբի դեմ պայքարի գլոբալ որևէ գործիքի ստեղծումը: Մինչ օրս զարգացած երկրները նախընտրում էին ամրապնդել ազգային օրենսդրությունը, զուգահեռաբար անցկացնելով փոստաղբի դեմ երկկողմանի կամ տարածաշրջանային մրցապայքար: Հաշվի առնելով իրենց անշահավետ դիրքը՝ որպես «գլոբալ հասարակական չարությունը» ստացողի, ինչն առավելապես ելնում է զարգացած երկրներից, զարգացող երկրների մեծ մասը շահագրգռված է փոստաղբի հիմնախնդրի համար գլոբալ պատասխանի մշակման հարցում:

Ծանոթագրություններ

1. «Համացանց» և «համաշխարհային սարդոստայն» (WWW) տերմիններն օգտագործվում են որպես հոմանիշներ, սակայն դրանց մեջ տարբերություններ կան: Համացանցը մի հսկայական ցանց է, որ ընդգրկում է մեծ թվով ցանցեր և բազմաթիվ տարբեր ծառայություններ է տրամադրում: «Համացանց» տերմինը երբեմն օգտագործվում է նշելու համար տեխնոլոգիաների ամբողջությունը՝ ենթակառուցվածքներից մինչև հավելվածները (էլեկտրոնային փոստ, FTP, WWW) և տեղադրված նյութերի բովանդակությունը: WWW-ն ընդամենը համացանցի հավելվածներից մեկն է, փաստաթղթերի համակարգ, որը արձանագրության օգնությամբ կապված է հիպերտեքստի փոխանցման հետ (HyperText Transfer Protocol, HTTP):

2. Էլեկտրացանցի միջոցով համացանցային թրաֆիկի փոխանցումը երբեմն անվանում են «համացանց վարդակից» (անգլալեզու տերմինն է Power Line Communication, PLC): Էլեկտրափոխանցման գծի օգտագործումը շատ օգտատերերի համար համացանցն ավելի հասանելի է դարձնում: Այդ տեխնոլոգիայի մասին լրացուցիչ տեղեկատվություն ստանալու համար տես «Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication" (Internet Society, ISOC Member Briefi ng No. 13: Համացանցային հասցեն՝ http://www.isoc.org/briefi ngs/013):

3. Առեւտրի համաշխարհային կազմակերպության (ԱՀԿ) մասնակից պետությունների հեռահաղորդակցային շուկաների ազատականացումը ձևականորեն հաստատվեց 1998 թ.՝ հեռահաղորդակցությունների մասին բազային համաձայնագրի շրջանակներում: Այդ համաձայնագրի ընդունումից հետո ավելի քան 100 պետություն սկսեց ազատականացման գործընթաց՝ կապված ազգային հեռահաղորդակցային մենաշնորհների հետ, ներմուծելով մրցակցություն և հաստատելով կարգավորման ազգային մեխանիզմներ: Ձևականորեն համաձայնագիրը կոչվում էր «Ծառայությունների առևտրի մասին գլխավոր համաձայնագրի չորրորդ արձանագրություն» (ընդունվել է 1996 թ. ապրիլի 30-ին, իսկ ուժի մեջ է մտել 1998 թ. փետրվարի 5-ին: Համացանցային հասցեն է՝ http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm):

4. WSIS-ի ընթացքում վիճելի հարցերից մեկը համացանցի կառավարման գործընթացներում ավելի ակտիվ մասնակցություն ունենալու ՀՄՄ-ի ձգտումն էր, հատկապես այն ճյուղերում, որոնք ICANN-ի պատասխանատվության ոլորտում են: Համացանցի վերաբերյալ ՀՄՄ-ի նախաձեռնությունների մասին ավելի շատ տես՝ http://www.itu.int/osg/spu/ip/:

5. Հեռահաղորդակցությունների բնագավառում ԱՀԿ-ի դերի մասին ավելի մանրամասն տես՝ http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm:

6. Տարածում է գտել այն կարծիքը, որ պետությունները տնտեսական մեծ շահույթներ կարող են ստանալ ազգային օպերատորների շուկայական մենաշնորհների արդյունքում: Այս տեսակետի հակառակորդները պնդում են, որ ազատականացումը թույլ է տալիս բարձրացնել ընդհանուր շուկայական գինը, այդպիսով, մենաշնորհային շուկայի համեմատ, բարձրացնելով պետության ստացած շահույթների մակարդակը:

7. Տարածաշրջանային գործող արձանագրային բաժիններ (RIR)՝ ARIN (համացանցի համարների արձանագրման ամերիկյան բաժին), APNIC (Ցանցային տեղեկատվության Ասիա-խաղաղօվկիանոսյան կենտրոն), LACNIC (Լատինական Ամերիկայի և Կարիբյան տարածաշրջանի IP հասցեների տարածաշրջանային արձանագրման բաժին), RIPE NCC (IP ցանցերի եվրոպական համակարգող կենտրոն, որն ընդգրկում է Եվրոպայի և Մերձավոր Արևելքի տարածաշրջանները) և AFRINIC (Ցանցային տեղեկատվության աֆրիկյան կենտրոն): Տարածաշրջանային արձանագրման համակարգերի գործառույթների առանձնահատկությունների մանրամասն նկարագրությունը տես՝ https://www.ripe.net/info/resource-admin/rir-system.html:

8. IPv6 արձանագրության շուրջ քննարկումների մասին մանրամասն տեղեկատվությունը հասանելի է «IP հասցեների և IPv6 բաշխում» հետազոտական նախագծի կայքում: Նախագիծն անցկացվել է 2005 թ. DiploFoundation «Համացանցի կառավարման

բնագավառում ներուժի ստեղծում» ծրագրի շրջանակներում: Հետազոտման հեղինակներն էին՝ Ժան Ֆիլեմոն Կիսանգուն և Մուենդե Նջիրաինին (Jean Philemon Kissangou, Marsha Guthrie, and Mwende Njiraini), (համացանցային հասցեն է՝ http://textus.diplomacy.edu/Textusbin/portal/Ghome.asp?IDspace=84):

9. Համացանցային արձանագրությունների անվտանգության հարցերի համալիր և տեխնոլոգիական բարձր մակարդակով կատարված ուսումնասիրություն, տես՝ Chris Chambers, Justin Dolske, and Jayaraman Iyer, TCP/IP Security, Department of Computer and Information Science, Ohio State University (համացանցային հասցեն՝ http://www.linuxsecurity.com/resource_files/documentation/tcpipecurity.html)

10. Վերին մակարդակի «ազգակցական» դոմենների համակարգի ամփոփումը տես՝ http://www.icann.org/registries/about.htm:

11. Ավելի վաղ ժամանակի դոմենի օրինակ, որն ստեղծվել է որոշակի բովանդակության նյութերի համար՝ kids.us դոմեն: ԱՄՆ Կոնգրեսն օրենք էր ընդունել kids.us դոմենի ստեղծման մասին, որը վերապահված էր մանկական տեղեկատվության համար: Հիմնական խնդիրն այն էր, թե ինչ բան է մանկական տեղեկատվությունը, որի վերաբերյալ պետք է որոշում ընդունվեր: Արդյունքում, կոնտենտի կարգավորման հետ կապված, կարող էին հակասություններ առաջանալ ինչպես տեսական, այնպես էլ գործնական մակարդակներում: Ներկայում kids.us դոմենը կիրառվում է բացառապես որպես ԱՄՆ երկրի դոմենի մի մաս:

12. .xxx դոմենի ստեղծման մասին վիճաբանությունների ժամանակ ԱՄՆ կառավարությունը չի պահպանել ICANN որոշումների ընդունման ընթացակարգերը: ԱՄՆ առևտրի նախարարությունն իր դժգոհությունն արտահայտել է ICANN տնօրենների խորհրդի ղեկավարին ուղղված նամակով:

13. .cat գոտում դոմենային անվան գրանցման համար դիմումի բլանկը տես՝ http://www.icann.org/tlds/stld-apps-19mar04/cat.htm:

14. Պաղեստինին ccTLD տրամադրելու մասին IANA հաշվետվությունը տես՝ http://www.IANA.org/reports/psreport22mar00.htm:

15. Օրինակ՝ ՀԱՀ-ը իր ինքնավարության իրավունքն օգտագործեց որպես հիմնավորում իր երկրի դոմենի վերահսկողությունը վերականգնելու համար: Վերջերս ընդունված օրենքը հռչակում է, որ ՀԱՀ կառավարության նշած սահմաններից դուրս երկրի դոմենի օգտագործումը համարվելու է հանցագործություն: Բազմակողմանի մոտեցման որպես հաջող օրինակ է, սովորաբար, բերվում ազգային դոմենների կառավարման բրազիլական մոդելը: Բրազիլական դոմենները կարգավորող ազգային մարմինը բաց է բոլոր հիմնական շահագրգիռ կողմերի համար, ներառյալ կառավարության մարմինները, բիզնեսը և քաղաքացիական հասարակությունը: Դրան հակառակ, Կամբոջայի փորձը, որտեղ ազգային դոմենի կառավարումը տրված է կառավարությանը, հաճախ անվանվում է լիազորությունների անհաջող փոխանցում: Կառավարությունը իջեցրել է ծառայությունների որակը և մտցրել է բարձր տուրքեր, ինչը բարդացրել է Կամբոջայի դոմենների գրանցումը: Ավելի մանրամասն տեղեկություններ ստանալու համար տես՝ Alfonso, Carlos, BR: CCTLD An Asset of the Commons, in: MacLean, Internet Governance: A Grand Collaboration (UN ICT Task Force, New York, 2004), pp. 291-299; Norbert Klein, Internet Governance: Perspectives from Cambodia in "Internet Governance: A Grand Collaboration" edited by Don MacLean (United Nations, 2004), pp. 227-237:

16. «Երկրի բարձր աստիճանի դոմենների պատվիրակների և վարչակարգերի սկզբունքները» ներկայում վերանայվում են, տես՝ http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm:

17. Արմատական գոտու սպասարկուների, ցանցին դրանց միացման կետերի և տեղագրության, ինչպես նաև կարգավորող կազմակերպությունների ցանկը տես՝ http://www.root-servers.org/:

18. Տես՝ http://www.icann.org/en/announcements/announcement-30sep09en.htm:

19. Այս և այլ դատական գործերի համառոտ շարադրանքը տես՝ http://www.diplomacy.edu/ig/resources/booklet/isp/:

20. Frances Williams, “ISPs should be liable for spam, says UN report” (Financial Times, 8 November 2006):

21. «Th e End user: Junk Payout in Spam Case», International Herald Tribune, 13 April 2006 (հասցեն համացանցում՝ http://www.iht.com/articles/2006/04/12/business/PTEND13.php).

22. HSCGroup-ի (www.hscgroup.co.uk) սահմանման համաձայն, պիրինգը «ցանցային օպերատորների միջև երկկողմանի համաձայնությունն է, որի նպատակը յուրաքանչյուր կողմի օգտատերերի դեպի մյուս կողմի ռեսուրսներ անվճար ներթափանցումն ապահովելն է»: Պիրինգի մասին պայմանագրերը ձեռնտու են բոլոր մասնակիցների համար և լայնորեն տարածված են համացանցի մատակարարների և հեռահաղորդակցային ցանցերի օպերատորների շրջանում:

23. 2-րդ աստիճանի համացանցի ծառայությունների մատակարարներին երբեմն անվանում են համացանցային անցախուցեր (Internet Gateways) կամ համացանցին միանալու կետեր (Internet Connection Points):

24. Էնդրյու Օդլիժկոն համացանցի գնագոյացման ու կառույցի հարցերը դիտարկում է պատմական հեռանկարում: Նա գնագոյացման ընդհանուր գծերը վեր է հանում սկսած Հին աշխարհի տրանսպորտային համակարգերից, այնուհետև զուգահեռներ է անցկացնում համացանցում ընթացող գնագոյացման քաղաքականության հետ: Տես՝ Andrew Odlyzko, «Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation» (համացանցային հասցեն՝ http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf).

25. Շոն Օ’Դոնելը «Համացանցի տնտեսական քարտեզը» հոդվածում բացատրում է, թե ուր են գնում համացանցի ծառայությունների մատակարարների օգտատերերի փողերը (Shawn O’Donnell. An Economic Map of the Internet: Համացանցային հասցեն՝ http://ebusiness.mit.edu/research/papers/162_ODonnell_Map.pdf), հղումը կատարել է Դյորդ Մարինկովիչը՝ Diplo’s Internet Governance Portal:

26. Th uy T. T. Nguyen and Grenville J. Armitage, “Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model,” ETRI Journal, vol.27, no.1, Feb. 2005, pp. 64-74.

27. Տես՝ http://www.bandwidthmarket.com վեբկայքը, որը համացանցի ռեսուրսների «առցանց շուկա է» համարվում, որով փոխանցման լայնագիծ ուղիներ, համացանց ներթափանցելու թույլտվություն և այլ ներուժեր են վաճառվում:

28. Geoff Huston, «Where’s the Money? –Internet Interconnection and Financial Settlements,» Th e ISP Column, Internet Society, January 2005 (համացանցային հասցեն՝ http://ispcolumn.isoc.org/2005-01/interconns.pdf).

29. «The Halfway Proposition: Background Paper on Reverse Subsidy of G8 Countries by African ISPs,» Conference of African Ministers of Finance, Planning and Economic Development, Johannesburg, South Africa, 19 October 2002.

30. Ներցանցային միացման արժեքի մանրամասն վերլուծությունը տես՝ B. Esmat and Juan Fernandez, “International Internet Connections Costs” in William J. Drake, “Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG),” New York: 2005, pp. 73-86. Mike Jensen, in “Interconnection Costs” (APC: 2005), հիմնախնդրի համալիր վերլուծությունը տես՝ http://rights.apc.org/ documents/interconnection_costs.pdf:

31. Geoff Huston, «Where’s the Money? Internet Interconnection and Financial Settlement,» Th e ISP Column, January 2005, Internet Society, pp. 7-9.

32. Միջպետական մակարդակով այդ հարցի համաձայնեցման ճանապարհին հանդիպող խոչընդոտներից մեկն այն փաստն է, որ միջցանցային միացման մասին համաձայնագրերի մեծ մասը կնքվում է մասնավոր ընկերությունների, հեռահաղորդակցային ցանցերի օպերատորների մակարդակով: Որպես կանոն, այդպիսի համաձայնագրերը գաղտնի են:

33. Թրաֆիկով փոխանակման տարածաշրջանային և ազգային կետերի ցանկը տես՝ http://en.wikipedia.org/wiki/List_of_Internet_exchange_points:

34. Աֆրիկայում թրաֆիկով կետերի փոխանակման հնարավորությունների մասին տեղեկությունը տես՝ «Internet Exchange Points: Th eir Importance to the Development of the Internet and Strategies for Th eir Deployment –The African Example», by Global Internet Policy Initiative (հասցանցային հասցեն՝ http://www.internetpolicy.net/practices/ixp.pdf)

35. «Կիբեռանվտանգության ոլորտում ՀՄՄ-ի գլոբալ օրակարգի» մասին ավելի մանրամասն տեղեկություն տես՝ http://www.itu.int/osg/csd/cybersecurity/gca/:

36. Պայմանագրի տեքստը տես՝ http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

37. Տվյալ գործիքների պաշտոնական անվանումն է՝ «Փոխադարձ իրավաբանական օգնություն ցուցաբերելու և քրեական հանցագործությունների մասին պայմանագրեր» (Mutual Legal Assistance in Criminal Matters Treaties, MLATs):

38. Can-Spam օրենքի մասին լրացուցիչ տեղեկատվություն տես՝ http://www.ft c.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm.

39. Փոստաղբի դեմ պայքարի գծով գերատեսչությունների կոնտակտային ցանցը (The Contact Network of Spam Enforcement Authorities CNSA) 2005 թ. հիմնադրել են 13 պետություն (Ֆրանսիան, Ավստրիան, Բելգիան, Կիպրոսը, Չեխիայի Հանրապետությունը, Դանիան, Հունաստանը, Իռլանդիան, Իտալիան, Լիտվան, Մալթան, Մեծ Բրիտանիան, Իսպանիան): Կազմակերպության նպատակն էր նպաստել մասնակից պետությունների միջև համագործակցության զարգացմանը և ԵՄ-ից դուրս ինստիտուտների, ինչպիսիք են՝ ՏՀՀԿ-ն և ՀՄՄ-ն, համաձայնեցմանը:

Բաժին 3

Իրավական տեսակետներ

Իրավական տեսակետներ

Համացանցի կառավարման բնագավառի համարյա ամեն մի հարցն ունի իրավական տեսակետներ, սակայն արագ զարգացող համացանցի համար իրավական բազայի ձևավորումը գտնվում է դեռևս նախնական փուլում: Գոյություն ունի համացանցի կառավարման իրավական տեսակետների երկու հիմնական մոտեցում՝ ա) «իրական» իրավունք: Սա մոտեցում է, որի շրջանակներում համացանցը որպես երևույթ է դիտարկվում, որը նման է իրեն նախորդած հեռահաղորդակցության տեխնոլոգիաներին (որոնք զարգացման ընթացքում՝ազդանշանային կրակից մինչև հեռախոս, երկար ճանապարհ են անցել): Համացանցը, թեև արագ է և մեծամասշտաբ, սակայն նախկինի պես հեռավորության վրա առանձին մարդկանց շփման միջոց է: Հետևաբար, գոյություն ունեցող յուրաքանչյուր իրավակարգ կարող է կիրառվել համացանցի նկատմամբ[1]: բ) «Կիբեռիրավունքը» ելնում է այն նկատառումներից, որ համացանցը ծնունդ է տվել կիբեռտարածության մեջ իրականացվող սոցիալական փոխհարաբերությունների նոր ձևերի: Հետևաբար, դրանց կարգավորման համար նոր «կիբեռօրենքներ» ձևակերպելու անհրաժեշտություն է առաջանում: Այս մոտեցմանը սատարող փաստարկն այն է, որ համացանցի օգնությամբ տարվող անհավանական արագությունն ու միջազգային շփման ծավալը խոչընդոտում են գոյություն ունեցող իրավակարգերի կիրառմանը: Երկու մոտեցումն էլ, թեև ճշմարտության հատիկ են պարունակում, այնուամենայնիվ, «իրականում» իրավունքը գերակշռում է և՛ տեսության մեջ, և՛ գործնականում: Առավել տարածում ունեցող կարծիքի համաձայն, գոյություն ունեցող օրենսդրության մեծ մասը կարող է կիրառվել համացանցի նկատմամբ: Սակայն իրական կյանքում գոյություն ունեցող իրավակարգերը մի շարք դեպքերում անհրաժեշտ է ձևափոխել, որպեսզի հնարավոր լինի դրանք կիրառել կիբեռտարածության նկատմամբ: Իսկ ավելի նեղ շրջանակի հիմնախնդիրների համար անհրաժեշտ է մշակել միանգամայն նոր օրենքներ:

Իրավական մեխանիզմներ

Գոյություն ունի իրավական մեխանիզմների լայն ընտրանի, որոնցից շատերը համացանցի կառավարման ոլորտում կամ արդեն կիրառվում են, կամ կարող են կիրառվել:

Պետական և սոցիալական իրավական մեխանիզմներ
Օրենսդրական կարգեր

Յուրաքանչյուր իրավակարգ ունի որոշակի դասավորություն (կանոն) և վավերացում: Դասավորությունը սահմանում է հասարակության մեջ ընդունված վարքի կանոնները (օրինակ՝ հանցագործություն չկատարել, վճարել հարկեր), իսկ վավերացումը սահմանում է պատիժ, որը սպառնում է կանոնները չպահպանելու դեպքում (օրինակ՝ տուգանքներ, ազատազրկում, որոշ երկրներում կիրառվում է նաև մահապատիժ): Համացանցի առնչությամբ օրենսդրական գործունեությունն աստիճանաբար ակտիվանում է: Այն հատկապես վերաբերում է ՏՀՀԿ անդամ երկրներին, որտեղ տեղեկատվական տեխնոլոգիաները լայնորեն տարածված են և մեծ ազդեցություն են գործում տնտեսական և սոցիալական հարաբերությունների վրա: Ներկայում օրենսդրական գործունեության առաջնային ճյուղերն են՝ մասնավոր կյանքի պաշտպանությունը, օգտատերերի մասին տվյալների պահպանումը, մտավոր սեփականության, հարկադրման, կիբեռհանցագործության դեմ հակազդեցության պաշտպանությունը: Սակայն սոցիալական հարաբերությունները բազմակողմանի են և չեն կարող կարգավորվել միայն օրենսդրությամբ: Հասարակությունն իր էությամբ հարաճուն է, և օրենսդրական կարգերը միշտ էլ հետ են մնում տեղի ունեցող փոփոխություններից: Այդ հատկապես նկատելի է մեր օրերում, երբ տեխնոլոգիական զարգացումը սոցիալական իրականությունն ավելի արագ է փոխում, քան օրենսդիրները կարող են արձագանքել այդ փոփոխություններին: Երբեմն, նույնիսկ, օրենքները հնանում են մինչ դրանց կիրառումը: Իրավական կարգերի այդ հնացման վտանգի մասին միշտ պետք է հիշել համացանցի կարգավորման գործընթացում:

Իրականը թե՞ «կիբեռմոտեցումը»

Անկախ այն բանից, թե մենք ինչն ենք ավելի համապատասխան համարում՝ «իրականը» թե «կիբեռմոտեցումը», մի բան անհերքելի է՝ օրենսդրական նորմերը հակաօրինական դրսևորումն անհնար չեն դարձնում, այլ ընդամենը պատիժ են սահմանում դրա համար: Այն փաստը, որ խարդախությունն արգելված է և իրական, և վիրտուալ աշխարհում, չի նշանակում, որ այն իսպառ կվերանա: Այս տարբերությունը կարևոր է, քանի որ հօգուտ «կիբեռաշխարհի» համար հատուկ իրավակարգեր մշակելու մասնավոր փաստարկներից մեկն այն հանգամանքն է, որ համացանցում հակաօրինական դրսևորումների տարբեր ձևերը (հանցագործություն, խարդախություն և այլն) շատ տարածված են, հետևաբար իրական կյանքի օրենքները չեն կարող արդյունավետորեն կիրառվել:

Սոցիալական կանոններ (սովորույթներ)

Օրինակարգերի պես սոցիալական կանոնները ևս արգելում են որոշակի գործելակերպ: Ի տարբերություն օրենսդրության, պետական ոչ մի հիմնարկություն լիազորված չէ պարտադրելու այդ կանոնների կատարումը: Դրանց կատարումը ապահովում է միությունը՝ անդամների մեկ մեկու վրա ազդեցություն գործելու միջոցով: Համացանցն իր պատմության արշալույսին գործնականում կարգավորվում էր բացառապես սահմանված սոցիալական կանոնների ամբողջությամբ, որն անվանվեց «նեթիկետ» (netiquette): Դրանք խախտելու համար սահմանված հիմնական պատիժը համացանցային միության մյուս անդամների գործադրած ճնշումն էր և միությունից նրանց հեռացնելը: Զարգացման այդ ժամանակաընթացքում, երբ համացանցից օգտվում էր մարդկանց համեմատաբար ոչ մեծ խումբ, հիմնականում՝ ուսումնասիրություններ կատարողները, ուսուցիչները և ուսանողները, սոցիալական կանոններն, ընդհանուր առմամբ, պահպանվում էին: Համացանցի աճը սոցիալական բնույթի կարգադրություններն անարդյունավետ դարձրեց: Կարգավորման այս տեսակը դեռևս կարող է կիրառվել, սակայն միայն լավ զարգացած ներքին կապեր ունեցող փակ խմբերում:

Ինքնակարգավորում

Համացանցի կառավարման վերաբերյալ 1998 թ. ԱՄՆ կառավարության կազմած «Սպիտակ գիրքը» համացանցի կառավարման գործում նախընտրությունը տալիս է ինքնակարգավորմանը: Ինքնակարգավորումն ընդգրկում է մի շարք տարրեր, որոնք բնութագրական են նաև վերը նշված սոցիալական նորմերի համար: Հիմնական տարբերությունն այն է, որ ի տարբերություն շատ հաճախ անորոշ արտահայտված սոցիալական նորմերի, ինքնակարգավորումը հիմնավորվում է լավ մտածված ու կազմակերպված մոտեցմամբ: Ինքնակարգավորման նորմերը, սովորաբար ամրապնդվում են պատշաճ վարքի օրենսգրքերում: Ինքնակարգավորման միտումը հատկապես լավ նկատելի է համացանցի մատակարարների շրջանում: Շատ երկրներում կառավարությունները ճնշում են գործադրում մատակարարների վրա, ձգտելով նրանց օգտագործել որպես համացանցի նյութերը քաղաքական կյանք մտցնելու գործիք: Մատակարարներն ավելի հաճախ են ապավինում ինքնակարգավորմանը՝ վարքի որոշակի ստանդարտներ հաստատելու համար և, վերջին հաշվով, կանխելու համար կառավարությունների միջամտություններն իրենց գործունեությանը: Ինքնակարգավորումը, թեև կարող է դառնալ օգտակար կանոնավորող գործիք, հենարան՝ հասարակայնության մեծ հետաքրքրությունն առաջացնող հարցերը լուծելիս (օրինակ՝ համացանցի նյութերի բովանդակության վերահսկողության քաղաքականություն վարողների համար), այնուամենայնիվ կապված է վտանգների հետ: Դեռևս

պարզ չէ, թե մատակարարները ինչ մակարդակով կարող են կարգավորել վեբկայքերում տեղադրված նյութերի բովանդակությունը: Նրանք կարող են, արդյոք, լիազորված իրավական ինստիտուտների փոխարեն որոշումներ ընդունել: Մատակարարներն արդյոք կարող են գնահատել, թե որն է ընդունելի բովանդակությունը: Այս համատեքստում չպետք է մոռանալ նաև համոզմունքների արտահայտման ազատության և մասնավոր կյանքի գաղտնիության մասին:

Դատական պրակտիկա

Դատական պրակտիկան (դատարանների որոշումները) ԱՄՆ-ի իրավական համակարգի կարևորագույն տարրն է, որի շրջանակներում ձեռնարկվեցին համացանցի կարգավորման առաջին փորձերը: Այդ համակարգում դատական նախադեպերը կարող են կիրառվել որպես օրենսդրական կարգեր, հատկապես այն դեպքերում, որոնք կապված են այնպիսի նոր հարցերի կարգավորման հետ, ինչպիսին է համացանցը: Դատավորները ստիպված են որոշումներ ընդունել նույնիսկ այն դեպքում, երբ իրենց տրամադրության տակ չունեն անհրաժեշտ իրավական կարգեր: Իրավական առաջին գործիքը, որին ձգտում են դատավորները, այն համանմանությունն է, որի դեպքում որևէ նոր բան կապվում է ինչ-որ ծանոթ բանի հետ: Համացանցի հետ կապված դատական գործերի մեծ մասը լուծվում է համանմանության օգնությամբ: Համանմանության ցանկը տրված է 30–35 էջերում:

Միջազգային իրավական կարգավորում

Միջազգային մասնավոր իրավունքի և միջազգային հանրային իրավունքի միջև տարբերությունը

Համացանցի կառավարման մասին քննարկումների ժամանակ հաճախ խոսվում է միջազգային իրավունքի վրա հիմնվելու անհրաժեշտության մասին: «Միջազգային իրավունք» տերմինը կիրառվում է որպես միջազգային հանրային իրավունք տերմինի հոմանիշ, որն ստեղծում են պետական ու միջկառավարական կազմակերպությունները՝ կնքելով միջազգային պայմանագրեր և համաձայնագրեր: Սակայն համացանցի հետ կապված իրավաբանական հիմնախնդիրների մեծ մասը, այդ թվում նաև պայմանագրային հարաբերություններն ու իրավախախտումները, ներառում են մասնավոր իրավունքի տարրեր: Այդպիսի հիմնախնդիրները լուծելիս անհրաժեշտ է կիրառել միջազգային մասնավոր իրավունքը: Միջազգային մասնավոր իրավակարգերի կիրառումը նախապես որոշվում է ազգային իրավակարգում, այլ ոչ միջազգային պայմանագրերում: Այդպիսի կարգերը սահմանում են չափանիշներ, որոնց հիման վրա սահմանվում է կիրարկվող

իրավասությունը և իրավական համակարգը՝ միջազգային տարրերով դատական գործերում (օրինակ՝ տարբեր երկրների երկու և ավելի անձանց միջև իրավական հարաբերություններ)[2]: Իրավասության և իրավական համակարգի ընտրության համար որպես չափանիշ է ծառայում մասնավոր անձի և ազգային իրավասության միջև կապը (օրինակ՝ ազգությունը, բնակության վայրը) կամ առանձին գործարքի և ազգային իրավասության միջև կապը (օրինակ՝ պայմանագիրը որտեղ է կնքվել, փոխանակումը որտեղ է տեղ գտել):

Միջազգային մասնավոր իրավունք

Համացանցի գլոբալ բնույթի արդյունքում լայն տարածում են գտել իրավական վեճերը, որոնց մասնակցում են տարբեր ազգային իրավասությունների ենթակա մասնավոր անձինք և ինստիտուտներ: Սակայն համացանցի հետ կապված դատական վեճերի լուծման համար միջազգային մասնավոր իրավունքը հազվադեպ է կիրառվում, հավանաբար այն պատճառով, որ դրանց ընթացակարգերը հաճախ բարդ են, դանդաղ են ընթանում և թանկ արժեն: Միջազգային մասնավոր իրավունքի հիմնական մեխանիզմները մշակվել են այն ժամանակ, երբ արտասահմանյան փոխգործողությունն այնքան տրածված ու արդյունավետ չէր, հետևաբար մասնավոր անձանց և կազմակերպությունների մասնակցությամբ դատական գործերը, որոնք տարբեր իրավասությունների էին վերաբերում, այնքան էլ շատ չէին:

Միջազգային հանրային իրավունք

Միջազգային հանրային իրավունքը կանոնակարգում է պետությունների միջև հարաբերությունները: Միջազգային հանրային իրավունքի որոշ գործիքներ արդեն կարգավորում են այնպիսի բարդ ոլորտներ, որոնք վերաբերում են համացանցի կառավարմանը (օրինակ՝ հեռահաղորդակցային կանոնակարգեր, մարդու իրավունքների վերաբերյալ պայմանագրեր, միջազգային առևտրային պայմանագրեր): Բաժնի այս մասում քննարկվելու են միջազգային հանրային իրավունքի միայն այն տարրերը, որոնք կարող են կիրառվել համացանցի կառավարման բնագավառում, այսինքն՝ միջազգային պայմանագրերն ու իրավական ավանդույթները, «փափուկ իրավունքը» և միջազգային իրավունքի հիմնական սկզբունքները (ius cogens):

Միջազգային պայմանագրեր

Համացանցին վերաբերող միջազգային հիմնական պայմանագրերն ընդունել է Հեռահաղորդակցության միջազգային միությունը: Հեռահաղորդակցության միջազգային կանոնակարգը 1998 թ. հեռահաղորդակցության կարգավորման սկզբունքների հիմքը դրեց, որոնք ներգործեցին

համացանցի հետագա զարգացման վրա: ՀՄՄ փաստաթղթերից բացի, միակ փաստաթուղթը, որն անմիջականորեն կարգավորում է համացանցում հարաբերությունները, ԵՄ-ի ընդունած Կիբեռհանցագործության մասին պայմանագիրն է: Սակայն միջազգային հանրային իրավունքի շատ այլ մեխանիզմներ կիրառելի են համացանցի կառավարման ավելի լայն տեսակետների կարգավորման համար, ինչպիսիք են՝ մարդու, առևտրի իրավունքները և մտավոր սեփականության իրավունքները:

Միջազգային սովորական իրավունք

Միջազգային սովորական իրավակարգի ձևավորումը ընդգրկում է երկու տարր՝ «ընդհանուր պրակտիկայի» առկայությունը (consuetudo) և այն որպես իրավաբանորեն պարտադիր ճանաչելը (opinio iuris): Սովորական իրավունքի զարգացումը երկար ժամանակ է պահանջում ընդհանուր պրակտիկայի «բյուրեղացման» համար: Նոր կանոնների որոշ տարրեր արդեն ձևավորվում են այն բանի հիման վրա, թե ԱՄՆ կառավարությունն ինչպես է իրականացնում համացանցի արմատական գոտու վերահսկողությունը: Համացանցի արմատական գոտու ֆայլում ազգային մատակարարների մասին գրառումների վարման հարցում ԱՄՆ կառավարությունը չմիջամտելու հետևողական քաղաքականություն է վարում: Այդպիսի կայուն պրակտիկան կարող է դառնալ սովորական իրավականոնների ձևավորման առաջին քայլը: Դեռևս չի կարելի պնդել, արդյոք ԱՄՆ գործողությունները հիմք են ընդունել որոշակի միջազգային իրավական կանոնները (opinio iuris): Այս ենթադրությունը եթե ճիշտ է, հնարավոր է, որ ձևավորվի միջազգային սովորական իրավունքի ճյուղ, որը կկանոնակարգի համացանցի արմատական սպասարկուների համակարգի մի մասի կառավարումը, որը վերաբերում է վերին մակարդակի ազգային մատակարարներին: Այդպիսի տրամաբանության տարածումը վերին մակարդակի «արմատական» մատակարարների (.com, .org, .edu, .net) իրավական կարգավիճակի վրա, որոնք կոնկրետ երկրների հետ կապ չունեն, հեշտ չի լինելու:

«Փափուկ իրավունք»

Համացանցի կառավարման մասին քննարկումների ընթացքում հաճախ է կիրառվում «փափուկ իրավունք» տերմինը: «Փափուկ իրավունքի» սահմանումների մեծ մասը մատնանշում է այն, ինչը չի ներկայացնում՝ դա իրավաբանորեն ոչ պարտադիր գործիք է: «Փափուկ իրավունքը» իավաբանական ուժ չունի, այդ պատճառով դրա կատարումը չեն կարող ապահովել միջազգային դատարանները կամ վեճերի լուծման այլ մեխանիզմները: «Փափուկ իրավունքի» գործիքները իրենցից ներկայացնում են սկզբունքներ և կարգեր, այլ ոչ որոշակի կանոններ: Սովորաբար դրանք ձևակերպված են լինում միջազգային այնպիսի փաստաթղթերում, ինչպիսիք են՝ հռչակագիրը, ղեկավար սկզբունքները և օրենսդրության օրինակները: WSIS-ի հիմնական ամփոփիչ փաստաթղթերը,

ներառյալ սկզբունքների հռչակագիրը, գործողությունների ծրագիրը և տարածաշրջանային հռչակագրերը, կարող են բազա դառնալ «փափուկ իրավունքի» կարգերի ստեղծման համար: Դրանք իրավաբանական ուժ չունեն, սակայն, որպես կանոն, երկարատև բանակցությունների և բոլոր երկրների միջև համաձայնության ձեռքբերման արդյունք են: Այն պարտավորությունները, որ պետությունները և այլ շահագրգիռ կողմերը կրում են «փափուկ իրավունքի» կարգերը քննարկելու և ընդհանուր համաձայնության գալու ընթացքում, հիմք են տալիս այդ փաստաթղթերը դիտարկելու որպես ավելին, քան դիտավորությունների մասին քաղաքական հռչակագրերն են[3]: «Փափուկ իրավունքը» համացանցի կառավարման հիմնախնդիրները լուծելիս մի շարք առավելությունների է տիրապետում: Նախ՝ այն ավելի պակաս ձևական մոտեցում է, որը պետություններից չի պահանջում պաշտոնական պարտավորություններ ընդունել, հետևաբար երկարատև բանակցությունների կարիք չունի: Երկրորդ՝ «փափուկ իրավունքի» գործիքները բավականին ճկուն են, ինչը նպաստում է նոր մոտեցումներ մշակելուն և հնարավորություն է տալիս համացանցի կառավարման բնագավառում արագորեն փոփոխվող իրավիճակներին հարմարվել: Երրորդ՝ բոլոր շահագրգիռ կողմերի մասնակցության տեսակետից «փափուկ իրավունքն» ավելի նպաստավոր է, քան ավանդական միջազգային-իրավական մոտեցումը, որը մասնակցության իրավունք է տալիս միայն պետություններին և միջկառավարական կազմակերպություններին:

Միջազգային իրավունքի հիմնական սկզբունքները (ius cogens)

Միջազգային պայմանագրերի իրավունքի մասին Վիեննայի պայմանագրում տրվում է ius cogens-ի հետևյալ սահմանումը. «Կարգ(եր), որը պետությունների միջազգային միությունները ն ընդունում և ճանաչում են, ընդհանուր առմամբ, որպես կանոն, որից որևէ շեղումն անթույլատրելի է, և որը կարող է փոփոխվել միայն միջազգային ընդհանուր իրավունքի հաջորդող կանոնի համաձայն, որն ունի նույնպիսի բնույթ»[4]: Բրիտանացի իրավաբան Իեն Բրաունլին ius cogens-ի օրինակարգերի հետևյալ օրինակներն է բերում. ուժի գործադրման արգելք, ցեղասպանության անթույլատրելիություն, ռասայական խտրականության անթույլատրելիության սկզբունք, մարդկության հանդեպ հանցագործությունների դատապարտում, ինչպես նաև ստրկավաճառությունն ու ծովահենությունն արգելող օրինակարգեր[5]: Համացանցը կառավարելիս ius cogens-ի օրինակարգերը կարող են հիմք դառնալ որոշակի կանոնների ընդհանրության ստեղծման համար, ինչպիսին է, օրինակ՝ համացանցում մանկական պոռնոգրական նյութերի տեղադրման արգելքը:

Իրավասություն

Համացանցի հետ կապված վեճերի թիվն անընդհատ ավելանում է, ինչն էլ իրավասությունը դարձնում է համացանցի կառավարման առավել նշանակալի ու վիճելի տեսակետներից մեկը: Իրավասության վերաբերյալ անորոշությունը կարող է ունենալ երկու անմիջական ու միաժամանակյա հետևանք.

-սեփական տարածքում սոցիալական փոխհարաբերությունների կարգավորման համար իր իրավական լիազորություններն իրականացնելու պետության անկարողությունը.

- արդարադատությունում իրենց իրավունքներն օգտագործելու ֆիզիկական և իրավաբանական առանձին անձանց անընդունակությունը (արդարադատությունից հրաժարվելը):

Հավանական այլ հետևանքներ կարող են դառնալ՝

-համացանցի իրավական ոչ անվտանգ լինելը, այդ թվում՝ պատասխանատվությունից խույս տալու և ավելի լավ իրավասություն ընտրելու հնարավորությունը.

-էլեկտրոնային առևտրի դանդաղ զարգացումը.

-համացանցի մասնատումը իրավաբանորեն անվտանգ գոտիների:

Ուշադրության արժանացնելով վերը նշված հետևանքները, եզրահանգում ենք, որ իրավասության ու դրա ընտրության ընթացակարգային հիմնավորումների հստակ սահմանումը համացանցի կառավարման տեսակետից ծայրաստիճան կարևոր հիմնախնդիր է:

Իրավասության և համացանցի միջև փոխադարձ կապը

Համացանցի և իրավասության փոխհարաբերություններն ի սկզբանե հակասական են, քանի որ իրավասությունը գլխավորապես հիմնավորվում է աշխարհը աշխարհագրորեն պետությունների տարանջատման վրա: Յուրաքանչյուր պետություն իրավունք ունի իր տարածքում ինքնիշխան իրավասություն իրականացնելու: Սակայն համացանցը հնարավոր է դարձնում սահմանից դուրս ակտիվ փոխգործողությունը, որին դժվար է (թեև կարելի է) հետևել կառավարության ավանդական մեխանիզմներով: Համացանցում իրավասության մասին հարցը մեզ կրկին հետ է տանում դեպի համացանցի կառավարման հետ կապված գլխավոր հիմնախնդիրներից մեկը՝ համացանցն ինչպես «ամրացնել» գոյություն ունեցող իրավական և քաղաքական քարտեզին:[6]

Իրավասություն՝ հիմնական տեսակետները

Իրավասությանը վերաբերող երեք հիմնական հարց գոյություն ունի.

-ո՞ր դատարանը կամ այլ պետական մարմինն ունի անհրաժեշտ լիազորություններ (դատավարական իրավասություն),

-ի՞նչ օրենքներ պետք է կիրառվեն (նյութական իրավասություն),

- ինչպե՞ս են կատարվում դատարանի որոշումները (գործադիր իրավասություն):

Ստույգ դեպքերում իրավասությունը որոշելու համար կիրառվում են հետևյալ հիմնական սկզբունքները.
-տարածքային սկզբունքը. սեփական տարածքում պետության իշխանությունը մարդկանց և սեփականության վրա.
-քաղաքացիության սկզբունքը. երկրի քաղաքացիների հանդեպ պետության իշխանությունը՝ անկախ նրանց գտնվելու վայրի (ազգության սկզբունքը).
-հետաքննության սկզբունքը. պետության սահմաններից դուրս տեղի ունեցած գործողությունների արդյունքում տվյալ պետության տարածքում դրսևորվող տնտեսական ու քաղաքական հետևանքները կարգավորելու պետության իրավունքը:
Արդի միջազգային իրավունքի հաստատած մեկ այլ կարևորագույն սկզբունք է համապարփակ իրավասությունը:[7] Այս իրավասության սկզբունքը նշանակում է, որ պետությունը իրավունք ունի որոշակի հանցագործություններ քրեորեն հետապնդել, անկախ այն բանից, թե որտեղ և ով է այն գործել, հաշվի չառնելով տարածքային, ազգային կամ պետական հատուկ շահերով կապերը:[8] Համապարփակ իրավասության ենթակա են այնպիսի իրավախախտումներ, ինչպիսիք են՝ ավազակային գործողությունը, զինվորական հանցագործությունները և ցեղասպանությունը:

Իրավասությունների բախումը

Իրավասությունների հաստատման սկզբունքները (տարածքային սկզբունք, ազգության սկզբունք և հետաքննության սկզբունք) անխուսափելիորեն ստեղծում են այնպիսի իրավիճակներ, երբ հատվում են մի քանի պետությունների դատարանների իրավասությունները: Իրավասությունները որոշելու առնչությամբ հիմնախնդիրներն առաջ են գալիս այն ժամանակ, երբ բախումն ունենում է արտատարածքային բաղադրիչ (օրինակ՝ դրան մասնակցում են տարբեր պետությունների քաղաքացիներ կամ գործի են դրվում միջազգային տարգործողություններ): Համացանցում տեղեկատվություն տեղադրելով, դժվար է համոզվել, որ դրանով հանդերձ չի խախտվում որևէ երկրի օրենսդրությունը: Համացանցում տեղադրված յուրաքանչյուր նյութի մասին տեղեկանալու թույլտվություն կարելի է ստանալ ամեն տեղից: Այդ իմաստով համացանցում իրականացվող գործունեության համարյա յուրաքանչյուր ձևն ունի միջազգային բաղադրիչ, ինչը կարող է տարբեր իրավասությունների կիրառման առիթ տալ և հասցնել, այսպես կոչված, «փոխներարկման ազդեցության» առաջացմանը[9]: Դատական գործերից ամենաակնառուն և շատ հաճախ հիշատակվողներից մեկը, որը լուսաբանում է իրավասության հիմնախնդիրը, 2001 թ. Ֆրանսիայում քննարկված Yahoo!-ի գործն է[10]: Այդ գործը հերթական անգամ ընդգծեց բազմաբանակ իրավասության հիմնախնդրի կարևորությունը[11]: Դատական հետաքննության պատճառը Yahoo! վեբկայքի թույլ տված նացիստական սրբությունների մասին Ֆրանսիայի օրենսդրության խախտումն էր, որն արգելում է այդպիսի բովանդակության

նյութերի ցուցադրումն ու վաճառքը: Նշենք, որ այդ վեբկայքը տեղակայված էր ԱՄՆ-ում, որտեղ նմանատիպ նյութերի տարածումը եղել և մնում է օրինական: Այս գործի առնչությամբ դատական որոշում ընդունվեց, որում կարգադրություն էր արվում տեխնիկական միջոցների օգտագործման մասին (երկրալոկացիոն ծրագրային ապահովում և թույլտվության իրավունքի զտում): Yahoo!-ին պարտավորեցրին գտնել Ֆրանսիայի օգտատերերին և ուղեփակել նրանց հասանելիության ուղին դեպի այն նյութերը, որոնք պարունակում են նացիստական բովանդակություն: Տեխնիկական որոշումներից բացի (երկրալոկացիոն ծրագրային ապահովումից և թույլտվության իրավունքի զտումից), իրավասությունների բախումը լուծելու մոտեցումները ներառում են օրենսդրության ազգային համակարգերի ներդաշնակումը և միջնորդ դատարանի ու վեճերի լուծման այլընտրանքային ուրիշ մեխանիզմների օգտագործումը:

Մանրամասն կիբեռանվտանգության և փոստաղբի վերաբերյալ բաժին 3-ում

Ազգային օրենքների ներդաշնակումը պետք է հանգեցնի համաշխարհային մակարդակով միասնական իրավակարգերի հավաքածուի ստեղծմանը: Եթե բոլոր երկրներում իրավակարգերը միանման լինեն, ապա իրավասության որոշման հարցը պետք է կորցնի իր սրությունը: Ներդաշնակումը կարող է լինել այն ոլորտներում, որտեղ արդեն ըստ հարկի գոյություն ունի միջազգային մակարդակով համաձայնություն, օրինակ՝ մանկական պոռնոգրաֆական նյութերի, ավազակության, ստրկության, ահաբեկչության և կիբեռհանցագործության վերաբերյալ: Աստիճանաբար մերձենում են տարբեր երկրների դիրքորոշումները նաև այլ հարցերի վերաբերյալ, ինչպիսիք են՝ փոստաղբն ու կիբեռանվտանգությունը: Սակայն որոշ ոլորտներում, ներառյալ համացանցի նյութերի բովանդակության վերահսկման քաղաքականությունը, գլոբալ համաձայնության հասնելու հավանականությունը քիչ է, քանի որ մշակութային հակասությունները գործուն աշխարհում ավելի կատաղի են, քան իրականում[12]: Անբավարար ներդաշնակման մեկ այլ հնարավոր հետևանք կարող է լինել համացանցի կարգավորման ցածր մակարդակ ունեցող երկրներում տեղեկատվական նյութերի տեղադրումը: Ծովային իրավունքի նմանությամբ, որոշ երկրներ կարող են դառնալ «հարմար դրոշներ»՝ համացանցի աշխարհում «օֆշորային» կենտրոնների համար:

Միջնորդ դատարան

Միջնորդ դատարանը (միջնորդական հետաքննություն) վեճերի լուծման մեխանիզմ է, որը կարող է օգտագործվել ավանդական դատական ընթացակարգերի փոխարեն: Միջնորդ դատարանի մեխանիզմը կիրառելիս որոշումներն ընդունում են մեկ կամ մի քանի մասնավոր անկախ անձինք, որոնց ընտրում են վեճի մասնակիցները: Միջազգային

առևտրային միջնորդ դատարանը մի հին ավանդույթ ունի: Միջնորդական հետաքննության մեխանիզմը, սովորաբար հաստատվում է կողմերի առանձին համաձայնությամբ, որոնք պայմանավորվում են հետագայում ծագած յուրաքանչյուր վեճ լուծել միջնորդ դատարանի օգնությամբ: Միջնորդ դատարանի մասին համաձայնագրերի շատ տարբերակներ գոյություն ունեն, որոնք կարգավորում են այնպիսի հարցեր, ինչպիսիք են՝ միջնորդական դատավարության անցկացման ընթացակարգը, կիրարկելի իրավունքի ընտրությունը և այլն: Ստորև բերվում է միջնորդ դատարանի և դատարանում վեճերի լուծման հիմնական տարբերությունների ամփոփումը:

Տարրեր	Դատական իրավասություն	Միջնորդ դատարան
Կազմակերպություն	Մշտական, սահմանվում է օրենքներով/ պայմանագրերով	Ժամանակավոր (ad hoc), սահմանում են մասնակիցները Մշտական՝ սահմանվում է պայմանագրերով
Կիրարկելի օրենքներ	Դատարանի իրավունքը (դատավորն ընդունում է որոշում՝ կիրարկելի օրենքի մասին)	Մասնակիցներն ընտրում են օրենքները. Հակառակ դեպքում օրենքները սահմանվում են համաձայնագրում, իսկ եթե համաձայնագրում օրենքները սահմանված չեն, կիրառվում են միջնորդական մարմնի օրենքները
Ընթացակարգեր	Դատական ընթացակարգերը սահմանվում են օրենքներով/ պայմանագրերով	Սահմանում են մասնակիցները (ad hoc): Սահմանում են միջնորդ դատարանի մարմինները (մշտական)
Իրավասություն/ վեճի առարկան	Սահմանվում են օրենքներով/ պայմանագրերով՝ համաձայն վեճի առարկայի	Սահմանում են մասնակցները
Որոշումներ	Պարտադիր	Պարտադիր

Միջնորդ դատարանն ի տարբերություն ավանդական դատարանների, շատ առավելություններ ունի, այդ թվում՝ մեծ ճկունություն, քիչ ծախսեր, արագություն, իրավասության ընտրության հնարավորություն, ինչպես նաև պետության սահմաններից դուրս ընդունված միջնորդական որոշումների ի կատար ածման պարզություն:

Միջնորդ դատարանի հիմնական առավելություններից մեկն այն է, որ այն չի լուծում ընթացակարգային և նյութական իրավասությունների ընտրության հիմնախնդիրը: Եվ մեկը, և՛ մյուսը նախօրոք ընտրում են վեճի մասնակիցները: Միջնորդ դատարանն ունի հատուկ առավելություններ նաև դատական գործերի առավել բարդ բաղադրիչում, որը կապված է համացանցի հետ՝ որոշումների ընդունման ապահովումը: Միջնորդ դատարանների որոշումների կատարումը կարգավորվում է Նյու Յորքի՝ օտարերկրյա միջնորդական որոշումների ընդունման և կատարման մասին պայմանագրով[13]: Այդ պայմանագրի համաձայն, ազգային դատարանները պարտավոր են կատարել միջնորդական որոշումները: Նյու Յորքի պայմանագրի իրավակարգի հիման վրա

միջնորդ դատարանների որոշումների կատարումն ավելի հեշտ է, քան սովորական դատական որոշումները: Միջնորդ դատարանը հաճախ օգտագործվում է առևտրային վեճերի լուծման ժամանակ: Ձևավորվել է հիմնավորապես մշակված կանոնների ու ինստիտուտների համակարգ, որն ուղղված է առևտրային վեճերի կարգավորմանը: Միջազգային հիմնական փաստաթուղթը միջազգային առևտրային միջնորդ դատարանի մասին տիպային օրենքն է, որը մշակվել է 1985 թ. UNCITRAL և լրացվել է UNCITRAL-ի իրավաբանական այլ գործիքներով[14]: Միջազգային միջնորդական առաջադեմ կազմակերպությունները, որպես կանոն, իրենց գործառույթները կատարում են առևտրային պալատներին կից և կարող են կազմակերպվել միջազգային (օրինակ՝ Միջազգային միջնորդ դատարան), տարածաշրջանային (օրինակ՝ Եվրոպական միջնորդ դատարան) և ազգային մակարդակով:

Միջնորդ դատարանն ու համացանցը

Միջնորդ դատարանը և վեճերի լուծման ուրիշ այլընտրանքային համակարգերը լայնորեն կիրառվում են՝ լրացնելու համար այն վակուումը, որն առաջանում է համացանցի հետ կապված գործերը վարելու գոյություն ունեցող միջազգային մասնավոր իրավունքի անկարողությունից: Միջնորդ դատարանի այդպիսի օգտագործման օրինակ է Դոմենային անունների մասին վեճերի քննարկման միասնական քաղաքականությունը (UDPR), որը մշակել է Մտավոր սեփականության միջազգային կազմակերպությունը (ՄՍՄԿ) և ընդունել է ICANN-ն՝ որպես վեճերի լուծման հիմնական ընթացակարգ[15]:

UDPR-ը ի սկզբանե բոլոր պայմանագրերում նշվում է որպես բախումների լուծման մեխանիզմ, կապված բարձր աստիճանի արմատական (.com, .edu, .org, .net) և ազգային որոշ դոմենների գրանցման հետ: Եզակի երևույթ է այն, որ միջնորդական որոշումները կիրառվում են անմիջականորեն դոմենային անունների համակարգում փոփոխություններ մտցնելով, առանց ազգային դատարանների մասնակցության:

Մանրամասն դոմենային անունների համակարգի վերաբերյալ բաժին 2-ում

Ընդհանուր առմամբ, կարելի է ասել, որ միջնորդ դատարանն իրենից ներկայացնում է բախումների լուծման ավելի արագ, պարզ և էժան միջոց: Սակայն համացանցում բախումները լուծելու համար որպես հիմնական մեխանիզմ դրա կիրառումը մի շարք էական թերություններ ունի: Նախ՝ քանի որ միջնորդ դատարանին դիմելուց առաջ կողմերի միջև նախնական համաձայնություն է լինում, ապա այս մեխանիզմը կիրառելի չէ դեպքերի այնպիսի լայն շրջանակի համար, երբ այդպիսի համաձայնություն կանխավ կնքել չի կարելի (զրպարտանք, կիբեռհանցագործություն): Երկրորդ՝ միջնորդ դատարանի մասին հոդվածները սովորական պայմանագրերում ներառելու գոյություն

ունեցող պրակտիկան շատերը դիտարկում են որպես թույլ կողմի համար ոչ ձեռնտու (սովորաբար համացանցի օգտատիրոջ կամ գնորդի համար՝ էլեկտրոնային առևտուր իրականացնելիս): Երրորդ՝ որոշ մարդկանց անհանգստացնում է այն փաստը, որ միջնորդ դատարանը նախադեպ ունեցող իրավունքը (ընկած է ԱՄՆ-ի և Մեծ Բրիտանիայի իրավական համակարգերի հիմքում) հասցնում է համաշխարհային մակարդակի, ինչը աստիճանաբար կհանգեցնի ազգային իրավական համակարգերի զսպման: Առևտրային իրավունքի առումով դա ավելի ընդունելի կարող է լինել, ուշադրության արժանացնելով արդեն գոյություն ունեցող նյութաիրավական կանոնների միասնականացման բարձր մակարդակը: Սակայն այնպիսի նուրբ ոլորտներում, ինչպիսին համացանցի նյութերի բովանդակությունն է, և սոցմշակութային տեսակետների առնչությամբ ազգային իրավական համակարգերը կարևոր են, քանի որ արտացոլում են իրենց երկրների մշակութային առանձնահատկությունները:

Մտավոր սեփականության իրավունք

Համաշխարհային տնտեսության մեջ գիտելիքն ու գաղափարը կարևորագույն ռեսուրսներ են: Որպես մտավոր սեփականության իրավունքների ձև դրանց պաշտպանությունը դառնում է համացանցի կառավարման կարևորագույն հարցերից մեկը: Մտավոր սեփականության իրավունքը գտնվում է նաև զարգացման վերաբերյալ քննարկումների կենտրոնում: Համացանցի զարգացումը մտավոր սեփականության իրավունքի վրա ազդել է հիմնականում գիտելիքների և տեղեկատվության «թվագրման», ինչպես նաև դրանց մշակման նոր հնարավորությունների ի հայտ գալու հետևանքով: Համացանցի հետ կապված հիմնախնդրի տեսակետները վերաբերում են առևտրային դրոշմանիշներին, հեղինակային իրավունքներին և արտոնագրերին[16]:

Հեղինակային իրավունք

Հեղինակային իրավունքը պաշտպանում է գաղափարների արտահայտումը միայն նյութականապես, օրինակ՝ գրքերի, խտասալիկների, համակարգչային ֆայլերի և այլնի ձևով: Գաղափարն ինքնին հեղինակային իրավունքով չի պաշտպանվում: Սակայն գործնականում երբեմն դժվար է տարբերակել գաղափարը և դրա արտահայտումը: Հեղինակային իրավունքների պաշտպանության կարգը համընթաց է տեխնոլոգիական առաջընթացին: Տեխնոլոգիական ամեն մի նոր գյուտ՝ տպագրական հաստոցը, ռադիոն, հեռուստացույցը, տեսամագնիտոֆոնը, ազդեցություն է գործել հեղինկային իրավունքի կիրառման ինչպես ձևի, այնպես էլ առանձնահատկությունների վրա: Համացանցն էլ բացառություն չէր: Համացանցային տեխնոլոգիաների զարգացումը՝ տեքստից մի հատված «կտրել և տեղադրելու»

հնարավորությունից մինչև ավելի բարդ գործողությունները, ինչպիսիք են համացանցով երաժշտական և տեսաֆայլերի անվճար տարածումը, մարտահրավեր էր հեղինակային իրավունքի ավանդական հայեցակարգին: Չարմանալի է, բայց համացանցը նոր հնարավորություններ է ստեղծում և՛ հեղինակային իրավունք ունեցողների համար՝ ապահովելով պաշտպանության ավելի հուսալի տեխնիկական միջոցներ, և՛ նյութերի օգտագործման մոնիտորինգի համար: Ծայրահեղ դեպքում հեղինակային իրավունք ունեցողները կարող են ընդհանրապես արգելել հեղինակային նյութերի նկատմամբ ներթափանցման իրավունքը, ինչն էլ հեղինակային իրավունքի հայեցակարգը անիմաստ կդարձնի: Այդ հնարավորությունները վտանգի են ենթարկում հեղինակների իրավունքների և հասարակական շահերի միջև եղած փխրուն հավասարակշռությունը, որն ընկած է հեղինակային իրավունքի հայեցակարգի հիմքում: Այսօր հեղինակային իրավունք ունեցողները, որոնց շահերը ներկայացնում են ձայնագրման և մուլտիմեդիա խոշոր ընկերությունները, իրենց իրավունքներն ավելի ակտիվորեն են պաշտպանում, քան շարքային օգտատերերը: Հասարակական շահերը դեռևս բավականաչափ հստակ չեն ձևակերպվում և ըստ արժանվույն չեն պաշտպանվում: Սակայն իրավիճակն աստիճանաբար շտկվում է, հիմնականում բազմաթիվ գլոբալ նախաձեռնությունների օգնությամբ, որոնք ուղղված են գիտության և տեղեկատվության մեջ ներթափանցելու ազատություն տրամադրելուն:

Արդի վիճակը

Ազգային և միջազգային մակարդակներում հեղինակային իրավունքի պաշտպանության ուժեղացումը

Ձվարճանքների և ձայնագրման արդյունաբերության ընկերությունները ազգային և միջազգային մակարդակներով անցկացնում են լոբբիստական ակտիվ գործունեություն՝ հօգուտ հեղինակային իրավունքների պաշտպանության ուժեղացման: ԱՄՆ-ում մտավոր սեփականության պաշտպանությունը ամրապնդվել է 1998 թ., «Թվայնացման ժամանակաշրջանում հեղինակային իրավունքների մասին» օրենքով (DMCA): Թվայնացված նյութերի պաշտպանությունը միջազգային մակարդակով 1996թ. ընդգրկվեց Մտավոր սեփականության համաշխարհային կազմակերպության (ՄՍՀԿ) հեղինակային իրավունքների պաշտպանության մասին պայմանագրում: Այդ պայմանագիրը նախատեսում է նաև հեղինակային իրավունքների պաշտպանության ռեժիմի խստացում, մասնավորապես, մտավոր սեփականության բացառիկ իրավունքների սահմանափակման դեպքերի համար ավելի խիստ պայմաններ, հեղինակային իրավունքների տեխնիկական պաշտպանության շրջանցումն արգելող և այլ նման միջոցներ:

Դատական գործերի քանակի աճ

2003 թ. համացանցային ծառայություններ մատակարարողներին ուղարկվել է դատարան ներկայանալու մոտավորապես 1000 ծանուցագիր՝ պահանջելով դադարեցնել իրենց հաճախորդների միջև ֆայլերի փոխանակումը, նաև հարուցվել է ավելի քան 500 քրեական գործ՝ անհատ օգտատերերի դեմ: Պիրինգային ցանցերում ֆայլերի փոխանակման համար ծրագրային ապահովում իրականացնող Grokster և StreamCast ընկերությունների դեմ հարուցված գործը հատկապես կարևոր է համացանցում հեղինակային իրավունքների ապագայի առումով: «Թվայնացման ժամանակաշրջանում հեղինակային իրավունքների մասին» օրենքի համաձայն, ԱՄՆ-ի ձայնագրման ընկերակցությունը պահանջում էր, որ այդ ընկերությունները դադարեցնեն այնպիսի տեխնոլոգիաների մշակումը, որոնք օգտատերերին թույլ են տալիս օրենքի խախտումով ֆայլեր փոխանակել: Սկզբում ԱՄՆ դատարանները ողջամտորեն որոշեցին հեղինակային իրավունքների հնարավոր խախտումների համար պատասխանատու չճանաչել այնպիսի ընկերություններին, ինչպիսիք են Grokster-ը և StreamCast-ն են: Սակայն 2005 թ. հունիսին ԱՄՆ Գերագույն դատարանը վճռեց, որ ծրագրային ապահովման մշակմամբ զբաղվողները պատասխանատվություն են կրում իրենց արտադրանքի ոչ ճիշտ օգտագործման համար:

Ծրագրային ապահովում՝ հեղինակային իրավունքների խախտումների դեմ

Օրենքը խախտողների կիրառած գործիքները կարող են օգտագործել նաև օրենքի պաշտպանները: Պետական իշխանություններն ու գործարար կառույցները ավանդաբար իրականացրել են իրենց գործառույթները՝ հիմնվելով իրավական մեխանիզմների վրա: Սակայն ակտիվորեն շրջանառվում են հեղինակային իրավունքների խախտման համար «այլընտրանքային» ծրագրային ապահովման կիրառումը: «International Herald Tribune»-ում հրապարակված հոդվածում թվարկվում է իրենց իրավունքները պաշտպանելու համար ձայնագրման և զվարճանքի ընկերությունների ծրագրային ապահովում օգտագործելու հետևյալ տարբերակները.

-«Տրոյացիներ» ծրագրեր, որոնք ուղարկվում են վեբկայքեր՝ օգտատերերին, որտեղ նրանք կարող են օրինական կերպով գնել այն երգը, որն անլեգալ կերպով փորձում էին բեռնել.

-ծրագրային ապահովում, որը որոշ ժամանակ ուղեփակում է համակարգիչը և էկրանին ցույց է տալիս նախազգուշացում՝ ավազակային (համակարգչահենային) երաժշտական ֆայլերի բեռնման մասին.

- «հանդարտ» ԾԱ-ն աննկատ սքան է անում կոշտ սկավառակը և փորձեր է անում դրա վրայից ավազակային ֆայլերը հեռացնելու.

-«արգելող» ԾԱ-ն ավազակային ֆայլերի բեռման փորձեր կատարելիս ուղեփակում է համացանց ներթափանցումը:

Սթենդֆորդի համալսարանի իրավաբանական ֆակուլտետի պրոֆեսոր Լորենս Լեսինգը նախազգուշացնում է, որ այդպիսի միջոցները կարող են հակաօրինական լինել: Նա ուշադրություն է դարձնում այն բանին, որ վերը նշված գործիքները ընդգրկված չէին հեղինակային իրավունքի խախտման դեմ պայքարի միջոցառումների «պաշտոնական» ցանկում: Արդյոք դա նշանակում է, որ այդպիսի միջոցներ կիրառող ընկերությունները խախտում են օրենքը:

«Թվային իրավունքների կառավարման» տեխնոլոգիաները

Հիմնախնդրի լուծման համար որպես երկարաժամկետ և ավելի կառուցողական մոտեցում յուրաքանչյուր գործ ներդնում է հեղինակային իրավունքով պաշտպանված նյութերի մատչելիության կառավարման տարբեր տեխնոլոգիաներ: Microsoft ընկերությունը ծրագրային ապահովում է ստեղծել «թվային իրավունքների կառավարման» համար, որի նպատակը ձայնային ֆայլերի, ֆիլմերի և հեղինակային իրավունքով պաշտպանված այլ նյութերի բեռնման կարգավորումն է: Նմանատիպ համակարգեր են ստեղծել նաև Xerox (ContentGuard), Philips և Sony (InterTrust) ընկերությունները: Հեղինակային իրավունքները պաշտպանելու համար տեխնոլոգիական գործիքների կիրառումը աժակցության է արժանացել ինչպես միջազգային մակարդակում (ՄՄՀԿ հեղինակային իրավունքի մասին պայմանագիր), այնպես էլ ԱՄՆ-ում ընդունված Թվայնացման ժամանակաշրջանում հեղինակային իրավունքների մասին օրենքում: Վերջինս, բացի այդ, հակաօրինական է համարել հեղինակային իրավունքների տեխնոլոգիական պաշտպանությունը շրջանցելու փորձերը:

Հարցեր

Հեղինկային իրավունքների պաշտպանության նոր մեխնիզմներ ստեղծել, թե՞ կատարելագործել գոյություն ունեցողները: Ինչպե՞ս պետք է փոխել հեղինակային իրավունքի մեխանիզմները, որպեսզի դրանք արտացոլեն այն մեծ փոփոխությունները, որ տեղի են ունենում թվային տեխնոլոգիների և համացանցի ոլորտում նվաճումների ազդեցության ներքո: «Սպիտակ գրքի» հեղինակների կարծիքով, ԱՄՆ կառավարությունը պետք է նվազագույն փոփոխություններ կատարի, հիմնականում «ապանյութականացման» ճանապարհով, «Մտավոր սեփականության և ազգային տեղեկատվական ենթակառուցվածքի մասին» օրենքի հեղինակային իրավունքի այնպիսի բազային հայեցակարգերում, ինչպիսիք են՝ արձանագրումը, տարածումը, փոխանցումը և հրապարակումը: Այդ մոտեցումն աջակցության է արժանացել հեղինակային իրավունքների պաշտպանության ոլորտի միջազգային հիմնական պայմանագրերում, ներառյալ մտավոր սեփականության իրավունքների առևտրային տեսակետների մասին պայմանագրերը (TRIPS) և հեղինակային իրավունքների մասին ՄՄՀԿ պայմանագիրը: Սակայն մեկ այլ տեսակետի կողմնակիցները գտնում են, որ իրավական համակարգում պետք է խորքային փոփոխություններ կատարվեն, քանի որ թվայնացման ժամանակաշրջանում հեղինակային իրավունքը ոչ միայն «պատճենումը կանխելու իրավունքն է», այլև «ներթափանցումը կանխելու իրավունքը»: Արդյունքում, հաշվի առնելով թվայնացված նյութեր ներթափանցելու սահմանափակման անընդհատ աճող հնարավորությունները, հարց է առաջանում՝ արդյոք, ընդհանրապես, պե՞տք է հեղինակային իրավունքը պաշտպանել: Անհրաժեշտ

է նաև հասկանալ, թե ինչպես պետք է իրականանա հասարակական շահերի պաշտպանությունը՝ հեղինակային իրավունքի պաշտպանությանը հավասարվող անհայտ երկրորդինը:

Հասարակական շահերի պաշտպանությունը. հեղինակային իրավունքով պաշտպանված նյութերի «բարեխիղճ օգտագործումը»

Հեղինակային իրավունքի պաշտպանության նպատակն ի սկզբանե եղել է ստեղծագործությունների և հայտնագործությունների խրախուսումը: Հենց այդ պատճառով այդ հասկացության մեջ են մտել երկու տարր՝ հեղինակների իրավունքների պաշտպանությունը և հասարակական շահերի պաշտպանությունը: Հիմնական բարդությունն այն էր, որ պետք էր լայն հասարակայնության համար նախատեսել հեղինակային իրավունքով պաշտպանված նյութեր մուտք գործելու հնարավորությունը, ի շահ ստեղծագործությունների խրախուսման, գիտելիքների ձեռք բերման և համընդհանուր բարեկեցության ապահովման: Այդ մեխանիզմի գործառույթի տեսակետից, հասարակական շահերը պաշտպանվում էին պահպանված նյութերի «բարեխիղճ օգտագործման» հայեցակարգի օգնությամբ: «Բարեխիղճ օգտագործում» հասկացությունը սովորաբար ընկալվում է որպես հետազոտությունների և այլ ոչ առևտրային նպատակների համար կիրառում:

Հեղինակային իրավունքների պաշտպանությունն ու զարգացումը

«Բարեխիղճ օգտագործման» յուրաքանչյուր սահմանափակում կարող է վատթարացնել զարգացող երկրների վիճակը: Համացանցը գիտության գլոբալ փոխանակմանը մասնակցելու համար հետազոտողներին, ուսանողներին և մյուս օգտատերերին, հատկապես զարգացող երկրների, հզոր գործիք է տրամադրում: Հեղինակային իրավունքների պաշտպանությունը սահմանափակող կարգը կարող է բացասական հետևանքներ առաջացնել զարգացող երկրների ներուժի համար: Մեկ այլ տեսակետ է զարգացող երկրների մշակույթի և արվեստի իրերի թվայնացման մասշտաբների աճը: Որքան էլ զարմանալի լինի, զարգացող երկրները, վերջիվերջո, հնարավոր է, որ վճարեն իրենց մշակութային և գեղարվեստական ժառանգության համար, երբ այն կթվայնացվի, կտեղադրվի նոր «փաթեթի մեջ» ու կդառնա արտասահմանյան զվարճալի և մեդիա ընկերությունների սեփականությունը:

Մտավոր սեփականության համաշխարհային կազմակերպությունը և մտավոր սեփականության իրավունքների առևտրային տեսանկյունների վերաբերյալ համաձայնագիրը

Մտավոր սեփականության (ՄՍ) իրավունքների պաշտպանության միջազգային երկու հիմնական կարգ գոյություն ունի: Մտավոր սեփականության համաշխարհային կազմակերպությունը (ՄՍՀԿ)

համակարգում է ՄՍ պաշտպանությունն ավանդական իմաստով՝ հիմված Բեռնի և Փարիզի պայմանագրերի վրա: Մեկ այլ, դեռևս նոր կազմավորվող կարգ է համակարգում Առեւտրի համաշխարհային կազմակերպությունը (ԱՀԿ) և հիմվում է մտավոր սեփականության իրավունքների առևտրային տեսանկյունների մասին համաձայնագրի (TRIPS) վրա: Միջազգային մակարդակով մտավոր սեփականության հարցերի համակարգումը ՄԱՀԿ-ից փոխանցվել է ԱՀԿ-ին՝ ՄՍ-ի պաշտպանպությունն ուժեղացնելու նպատակով, հատկապես իրավակիրառման տեսանկյունից: Այս հանգամանքը զարգացած երկրների հիմնական նվաճումը դարձավ ԱՀԿ բանակցությունների ուրուգվայական փուլի ժամանակ: Զարգացող շատ երկրների անհանգստացնում են այդ իրադարձությունները: ԱՀԿ շրջանակներում գոյություն ունեցող իրավապահ խիստ մեխանիզմները կարող են սահմանափակել զարգացող երկրների խուսավարուման տարածությունը և զարգացման պահանջարկի ու մտավոր սեփականության միջազգային (հիմնականում ամերիկյան) իրավունքների միջև հավասարակշռություն գտնելու հնարավորությունը: Մինչ օրս ԱՀԿ և TRIPS կիզակետում էին դեղագործական ապրանքների վերաբերյալ մտավոր սեփականության իրավունքների տարբեր մեկնաբանություններ: Միանգամայն հնարավոր է, որ ապագայում քննարկման առարկա կդառնա մտավոր սեփականությունն ու համացանցը:

Համացանցային ծառայություններ մատակարարողների պատասխանատվությունը՝ հեղինակային իրավունքը խախտելու համար

Մտավոր սեփականության բնագավառում միջազգային իրավապահպանման մեխանիզմների խստացմանն ուղղված ևս մեկ քայլ դարձավ համացանցային ծառայություններ մատակարարողների պատասխանատվությունը՝ իրենց սպասարկման համակարգչում հեղինակային իրավունքը խախտող նյութեր տեղադրված լինելու համար (եթե այդպիսի խախտման մասին ծանուցումից հետո նման նյութերը չեն հեռացվում): Դրա շնորհիվ մտավոր սեփականության իրավունքների պաշտպանությունն անմիջականորեն համացանցում ապահովելու հնարավորություն ստեղծվեց:

Առևտրային անվանանիշի պաշտպանությունը

Առևտրային անվանանիշերի պաշտպանության տեսանկյունից հիմնախնդիրը դոմենային անունների գրանցումը կարգավորելն է: Համացանցի զարգացման սկզբնական շրջանում դոմենային անուն էր տրվում նրան, ով առաջինն էր դրա համար հայտ ներկայացնում: Դա հանգեցրեց,այսպես կոչված, գործնական կիբեռսքվոթինգի, այսինքն՝ ընկերությունների անվանումների գրանցումը՝ որպես դոմենային անուններ և դրանց հետագա վերավաճառքն ավելի բարձր գնով: Այդ իրավիճակը

բիզնեսի ներկայացուցիչներին ստիպեց համացանցի կառավարման բարեփոխումներում առևտրային անվանանիշերի պաշտպանության մասին հարցը համարել գլխավոր, ինչն էլ հանգեցրեց այն բանին, որ 1998 թ. ստեղծվեց Համացանցում անունների և համարների շնորհման միությունը (ICANN): «Սպիտակ գրքում», որի հիման վրա ստեղծվեց ICANN-ը, ԱՄՆ կառավարությունը կազմակերպության առջև խնդիր էր դրել առևտրային անվանանիշերի պաշտպանության մեխանիզմ մշակել և այն կիրառել դոմենային անունների ոլորտում: ICANN-ը իր ստեղծումից շատ չանցած ներկայացնում է դոմենային անունների վերաբերյալ վեճերի քննարկման միասնական քաղաքականություն (UDPR), որը մշակել էր Մտավոր սեփականության համաշխարհային կազմակերպությունը[17]:

Արտոնագրեր

Արտոնագիրը, ըստ ավանդության, գլխավորապես տեխնիկայի կամ արտադրության բնագավառում պաշտպանում է նոր գործընթացը կամ արտադրանքը: Միայն վերջերս են սկսել արտոնագրեր տալ ծրագրային ապահովման համար: Գրանցված արտոնագրերի քանակի աճի համապատասխան առաջ են գալիս մեծ փողերի հետ կապված դատական գործեր՝ ամերիկյան ընկերությունների՝ ԾԱ արտադրողների անմիջական մասնակցությամբ: Բիզնեսային գործընթացների պաշտպանության համար գրանցված արտոնագրերից մի քանիսը խիստ վիճելի էին, օրինակ՝ British Telecom-ի պահանջն այն մասին, որ իրեն վճարեն 1980 թ. գրանցված հիպերտեքստային հղումների արտոնագրման լիցենզավորված հատուցում: 2002թ. Օգոստոսին հայցը մերժվում է[18]: Եթե British Telecom-ը այդ դատական գործը շահեր, ապա համացանցի օգտատերերը ստիպված պետք է վճարեին յուրաքանչյուր հղման համար: Կարևոր է ընդգծել, որ ԾԱ և համացանցի հետ կապված ընթացակարգերի համար արտոնագրերի հանձնման պրակտիկան աջակցություն չի գտնում ոչ Եվրամիությունում, ոչ էլ երկրների մեծ մասում[19]:

Կիբեռհանցագործություն

«Իրական» և «վիրտուալ» իրավունքների միջև հակասություններ գոյություն ունեն նաև այս հարթության վրա: «Իրական» իրավունքի կողմնակիցներն ընդգծում են, որ կիբեռհանցագործությունը նման է «առցանց» աշխարհում կատարվող հանցանքներին, միայն մի տարբերությամբ, որ սովորաբար կատարվում է, որպես կանոն, համացանցին միացած համակարգչի օգնությամբ: Հանցագործությունները նույնն են լինում, միայն դրանց գործելու միջոցներն են տարբերվում: «Կիբեռմոտեցման» համաձայն, կիբեռհանցագործության եզակի տարրերը հատուկ մոտեցում են պահանջում, հատկապես, երբ խոսքը վերաբերում է օրենքի կիրառմանը և հանցագործության կանխմանը:

Կիբեռհանցագործության վերաբերյալ ԵԽ պայմանագիր կազմողները հակված էին դեպի «իրական» իրավունքը, ընդգծելով, որ կիբեռհանցագործության միակ առանձնահատկությունն այն է, որ հեռահաղորդակցային տեխնոլոգիաներն օգտագործում են որպես հանցագործություն կատարելու միջոց: Պայմանագիրն ուժի մեջ մտավ 2004 թ. հուլիսի 1-ին և այդ բնագավառի հիմնական գործիքն է համարվում[20]:

Հարցեր

Կիբեռհանցագործության սահմանումը

«Կիբեռհանցագործություն» հասկացության սահմանումը «կիբեռիրավունքի» կարևոր հարցերից մեկն է, որն ունի գործուն իրավական նշանակություն: Հենց սահմանումից է կախված, թե ինչպիսի իրավախախտումներ են վերաբերելու կիբեռհանցագործությանը: Եթե սահմանումը կենտրոնանալու է համակարգչային համակարգերի դեմ կատարված հանցագործությունների վրա, ապա կիբեռհանցագործությունը ընդգրկելու է՝ հեղինակի հավանությանը չարժանացած ներթափանցման իրավունքը, համակարգչային տվյալներին կամ ծրագրերին հասցրած վնասը, համակարգչային համակարգի կամ ցանցի նորմալ գործառույթը խախտելու նպատակով կատարված գործադուլը, հեղինակի հավանությանը չարժանացած, համակարգի միջոցով փոխանցվող, ստացվող կամ դրանում պահվող տվյալների զավթումը, ինչպես նաև համակարգչային լրտեսությունը: Ինչպես համացանցի կամ համակարգչային համակարգերի օգնությամբ կատարված յուրաքանչյուր հանցագործության, այնպես էլ կիբեռհանցագործության սահմանումն ընդգրկում է իրավախախտումների ավելի լայն սպեկտր, այդ թվում նաև կիբեռհանցագործության մասին պայմանագրում նշվածները, ինչպիսիք են՝ համակարգչային խարդախությունը, հեղինակային իրավունքների խախտումը, մանկական պոռնոգրական նյութերը, ինչպես նաև ցանցերի անվտանգության խախտումը:

Կիբեռհանցագործությունն ու մարդու իրավունքների պաշտպանությունը

Կիբեռհանցագործության մասին պայմանագիրը սրեց անվտանգության և մարդու իրավունքների միջև հավասարակշռության մասին բանավեճը: Երկյուղ կա և, հիմնականում, քաղաքացիական հասարակության մոտ, որ պայմանագիրն իշխանություններին չափից ավելի արտոնություններ է տալիս, ընդհուպ համակարգչահենների համակարգիչները ստուգելու իրավունքը, տեղեկատվության փոխանակմանը հետևելը և այլն: Այդ մեծ արտոնությունները կարող են վտանգի ենթարկել մարդու որոշ իրավունքներ, մասնավորապես, մասնավոր կյանքի իրավունքը և համոզմունքների

արտահայտման ազատությունը[21]: Կիբեռհանցագործության մասին պայմանագիրն ընդունել է Եվրախորհուրդը՝ միջազգային ակտիվ կազմակերպություններից մեկը, որ հանդես է գալիս ի պաշտպանություն մարդու իրավունքների: Այս հանգամանքը կարող է նպաստել, որպեսզի գտնվի կիբեռհանցագործության դեմ պայքարի և մարդու իրավունքների պաշտպանության միջև անհրաժեշտ հավասարակշռությունը:

Հանցանշանների հավաքագրումն ու պահպանումը

Կիբեռհանցագործության դեմ պայքարի հիմնական բարդություններից մեկը դատական գործ վարելու համար տվյալների հավաքագրումն է: Արդի հեռահաղորդակցությունների արագությունը իրավապահ մարմիններից արագ հակազդեցություն է պահանջում: Հանցանշանների պահպանման հնարավոր միջոցներից մեկը համացանցային մատակարարների կողմից էլեկտրոնային արձանագրությունների (լոգ) վարումն է, որոնցում գրանցվում է տեղեկատվություն այն մասին, թե ով և երբ է այս կամ այն ռեսուրս ներթափանցելու իրավունք ստացել: Կիբեռհանցագործության մասին պայմանագրի որոշ դրույթներ սահմանում են համացանցային թրաֆիկի մասին տվյալների պահպանման պարտավորություն: Իրավական այս նորմը համացանցում իրավակարգ ապահովելու գործում կարող է ազդեցություն ունենալ համացանցային ծառայություններ մատակարարողների դերի վրա:

Աշխատանքային օրենսդրություն

Հաճախ են խոսում այն մասին, որ համացանցը փոխում է աշխատանքային գործունեության բնույթը: Այս երևույթը, թեև մանրամասն քննարկում է պահանջում, սակայն անմիջականորեն համացանցի կառավարման համար մեծ կարևորություն ունեն հետևյալ տեսակետները.

-համացանցի շնորհիվ ավելացել է ժամանակավոր և կարճաժամկետ աշխատողների թիվը: Ի հայտ է եկել «մշտական ժամանակավոր» տերմինը, որով մատնանշում են այն աշխատակիցներին, ում միշտ պահում են կարճաժամկետ, բայց կանոնավոր կերպով թարմացվող պայմանագրերի կնքմամբ: Դա հանգեցնում է աշխատակիցների սոցիալական պաշտպանվածության նվազման:

-Հեռահաղորդակցության անընդմեջ զարգացման և համացանցի լայնաշերտ հասանելիության տարածման հետ ավելի ու ավելի մեծ տարածում է գտնում հեռավորությունից կազմակերպվող աշխատանքը (այսպես կոչված՝ հեռաշխատանքը):

-Ավելի է կարևորվում տեղեկատվական տեխնոլոգիաների հետ կապված սպասարկման ոլորտի աշխատանքի մի մասը (call-կենտրոնները, տվյալների մշակման բաժինները) անընդմեջ այլ երկրներ փոխանցելու միտումը: Այդպիսի աշխատանքի մի մեծ ծավալ արդեն ուղարկվել է Ասիայի և Լատինական Ամերիկայի երկրներ, որտեղ աշխատուժի արժեքն այնքան էլ բարձր չէ:

Տեղեկատվական տեխնոլոգիաների զարգացումը խախտեց աշխատանքի, ազատ ժամանակի և քնելու (8 + 8 + 8 ժամ) սովորական հերթագայությունը: Ավելի ու ավելի է դժվարանում որոշելը, թե երբ է սկսվում և երբ ավարտվում աշխատանքը: Սովորությունների այս փոփոխությունները կարող են պարտադրել, որպեսզի աշխատանքային նոր օրենսդրություն ստեղծվի, որը կկարգավորի այնպիսի տեսակետներ, ինչպիսիք են՝ աշխատանքային ժամանակի տևողությունը, աշխատողների շահերի պաշտպանությունը և աշխատավարձը: Աշխատանքային օրենսդրության կարևորագույն տեսանկյունը աշխատավայրում մասնավոր կյանքի գաղտնիության մասին հարցն է: Գործատուն, արդյոք, իրավունք ունի՞ հետևելու, թե իր աշխատակիցները համացանցից ինչպես են օգտվում (ստուգել էլեկտրոնային հաղորդագրությունների բովանդակությունը կամ վերահսկել նրանց մուտքը կայքեր): Օրենսդրությունը զարգանում է նաև այս ոլորտում, ի հայտ են գալիս բազմազան նոր որոշումներ: Ֆրանսիայում, Պորտուգալիայում և Մեծ Բրիտանիայում իրավական կանոններն ու դատական որոշ գործեր պաշտպանում են աշխատողին՝ սահմանափակելով աշխատակիցների էլեկտրոնային նամակագրությանը հետևելու գործատուի իրավունքը: Այդպիսի միջոցներ ձեռնարկելու մասին գործատուն պարտավոր է նախապես զգուշացնել իր աշխատակիցներին: Դանիայի դատարանը քննել է էլեկտրոնային անձնական նամակներ ուղարկելու և սեքսուալ թեմաներով ակնթարթային հաղորդակցման (չաթի) համար աշխատակցին աշխատանքից հեռացնելու մասին մի գործ: Դատարանը որոշում է կայացրել, որ հեռացումն անօրինական է, քանի որ գործատուն պաշտոնական քաղաքականություն չի վարել այն մասին, որ արգելվում է աշխատավայրում անձնական նպատակներով համացանցն օգտագործել: Հօգուտ աշխատակցի մեկ այլ փաստարկ էր այն, որ համացանցն օգտագործելը չէր ազդել նրա աշխատանքի որակի վրա: Աշխատանքային օրենսդրությունը, ըստ ավանդության, համարվում է ներպետական: Սակայն համաշխարհայնացումն ու համացանցի զարգացումը հանգեցրին աշխատանքային օրենսդրությանը վերաբերող հարցերի միջազգայնացմանը: Ուշադրության արժանացնելով արտասահմանյան կազմակերպություններում աշխատող մարդկանց թվի աճը և միջազգային մակարդակով իրականացվող փոխգործողությունները, հարկ է ընդունել, որ արդեն հասունացել է կարգավորման համապատասխան միջազգային մեխանիզմների ստեղծման անհրաժեշտությունը: Այս տեսանկյունն ընդունվել է WSIS հռչակագրում, որի 47 կետը կոչ է անում հարգել աշխատաշուկայում տեղեկատվական տեխնոլոգիաների հետ կապված համապատասխան միջազգային նորմերը:

Ծանոթագրություններ

1. Իրական մոտեցման կողմնակիցներից մեկը ամերիկացի դատավոր Ֆրենկ Իսթերբրուկն է, ում էլ վերագրում են հետևյալ խոսքերը. «Անհոգ եղեք, կիբեռիրավունք գոյություն չունի»: «Կիբեռտարածությունն ու ձիու իրավունքը» հոդվածում նա հայտարարում է, որ չնայած ձիերի կարևորությանը, ձիերի իրավունք՝ որպես առանձին ոլորտ, երբևէ գոյություն չի ունեցել: Իսթերբրուկը պնդում է, որ անհրաժեշտ է հիմնվել իրավական բազային այնպիսի գործիքների վրա, ինչպիսիք են՝պայմանագրերը, պարտավորությունները և այլն: Տես՝ Frank H. Easterbrook. Cyberspace and the Law of the Horse. University of Chicago Legal Forum Issue 207, 1996 (համացանցային հասցեն՝

http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdf).

Ֆրենկ Իսթերբրուկի փաստարկները մեծ հնչեղություն ունեցան, միաժամանակ բանավեճ սկսեց Լորենս Լեսիգը: Տես՝ Lawrence Lessig. Th e Law of the Horse: What Cyberlaw Might

Teach (համացանցային հասցեն՝http://www.lessig.org/content/articles/works/fi nalhls.pdf):

2. Ներկայում մի քանի փորձեր են արվել ներդաշնակելու միջազգային մասնավոր իրավունքը: Գլոբալ հիմնական ֆորումը Միջազգային մասնավոր իրավունքի վերաբերյալ Հաագայի համաժողովն է, որն այդ բնագավառում բազմաթիվ պայմանագրեր է մշակել և ընդունել:

3. WSIS փաստաթղթերում հաճախ է հանդիպում «հետևում է» բառը, որը «փափուկ իրավունքի» առանձնահատկությունն է: Ավելի մանրամասն տեղեկություններ ստանալու համար տես՝ Jovan Kurbalija, Th e Emerging Language of ICT Diplomacy– Qualitative Analysis of Terms and Concepts, DiploFoundation.

4. 1969 թ. միջազգային պայմանագրերի մասին Վիեննայի պայմանագրի 53-րդ հոդված:

5. Ian Brownlie, Principles of Public International Law, 5th Ed. (Oxford: Oxford University Press, 1999), p. 513.

6. Ավելի մանրամասն տեղեկատվություն ստանալու համար տես՝ Richard Paul Salis, A Summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: «Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet», (համացանցային հասցեն՝ http://www.lex-electronica.

org/articles/v7-1/Salis.htm); Jonathan Zittrain, Jurisdiction in Cyberspace, Internet Law Program (համացանցային հասցեն՝ http://cyber.law.harvard.edu/ilaw/mexico_2006_

module_9_jurisdiction); Jurisdiction Over Internet Disputes: Diff erent Perspectives Under American and European Law in 2002, ABA Section on International Law and Practice. Annual Spring Meeting, New York City, May 8, 2002 (համացանցային հասցեն՝ http://www.howardrice.com/uploads/content/jurisdiction_internet.pdf).

7. Այդ բնագավառի առավել կարևոր ռեսուրսներից է «Համապարփակ իրավասության փրինսթոնյան սկզբունքները» (Princeton Principles on Universal Jurisdiction) 2001 ր. (համացանցային հասցեն՝ http://www1.umn.edu/humanrts/instree/princeton.html):

8. Peter Malanczuk, Akehurst's Modern Introduction to International Law (London: Routledge, 1997), p. 113.

9. Համացանցի նյութերի բովանդակությանը վերաբերող էքստրատարածքային իրավասության դատական գործերի ամփոփում: Տես՝ Yulia A. Timofeeva, Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis, Connecticut Journal of International Law, 20, p. 199, 2005 (համացանցային հասցեն՝ http://ssrn.com/abstract=637961):

10. Բացի այդ, դատական հայցերն ընդգրկում են Գերմանիայի դաշնային դատարանի գործն ընդդեմ Ավստրիայի քաղաքացի, նախկինում Գերմանիայի քաղաքացի Ֆրեդերիկ Տոբենի, ով վիճարկում էր Հոլոքոսթի գոյության մասին Ավստրիայի վերկայքում: Տես՝ http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html:

11. Տեղեկատվություն դատական հետագա գործընթացի մասին տես՝ http://www.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo:

12. Վիճելի իրավիճակները կապված են ոչ միայն ռասիստական կամ պոռնոգրաական նյութերի հետ, դրանց հետ միասին տարբեր վերաբերմունք են առաջացնում անօրինական մոլի խաղերը, ծխախոտի և թմրանյութերի վաճառքի մասին գովազդը:

13. Պայմանագրի ամբողջական տեքստը տես՝ http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html:

14. UNCITRAL գործիքներն ընդգրկում են նաև Միջնորդ դատարանի UNCITRAL 1976 թ.ընթացակարգը, UNCITRAL 1980 թ. համաձայնեցման ընթացակարգը, 1996 թ. միջնորդական հետաքննության կազմակերպման մասին UNCITRAL մեկնաբանությունները, 2002 թ. Միջազգային առևտրային համաձայնեցման ընթացակարգի մասին UNCITRAL Մոդելային օրենքը:

15. Uniform Domain Name Dispute Resolution Policy, The Internet Corporation for Assigned Names and Numbers, 26 August 1999 (համացանցային հասցեն՝ http://www.icann.org/udrp/udrp-policy-24oct99.htm).

16. Բացի այդ, մտավոր սեփականության հանդեպ իրավունքները տարածվում են արդյունաբերական նմուշների, օգտակար մոդելների, առևտրային գաղտնիքների, աշխարհագրական նշումների և բույսերի տեսակների վրա:

17. Այն հիմնախնդիրների համապարփակ վերլուծությունը, որոնց հետ բախվում է UDPR-ն, տես՝ «WIPO's Overview of WIPO Panel Views on Selected UDRP Questions» (համացանցային հասցեն՝ http://arbiter.wipo.int/domains/search/overview/index.html):

18. CNET News.com. Loney, M., «Hyperlink patent case fails to click» (համացանցային հասցեն՝ http://news.com.com/2100-1033-955001.html):

19. Եվրոպայում ԾԱ արտոնագրման հարցի քննարկումների մասին ավելի մանրամասն տեղեկատվություն տես՝ http://swpat.ffi i.org և ttp://www.eubusiness.com/Rd/patents.2006-02-02:

20. Պայմանագրի ամբողջական տեքստը տես՝ http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm:

21. Կիբեռհանցագործության մասին քննադատական կարծիք, որն արտահայտում է մարդու իրավունքների պաշտպանությամբ հադես եկող քաղաքացիական հասարակության և շարժումների մտահոգությունը, տես՝ The Association for Progressive Communication Report on the Cybercrime Convention: http://rights.apc.org/privacy/treaties_icc_bailey.shtml; վեբկայք՝ TreatyWatch.org http://www.treatywatch.org:

Բաժին 4

Տնտեսական տեսակետներ

Տնտեսական տեսակետներ

Վերջին տասնամյակի ընթացքում էլեկտրոնային առևտուրը համացանցի զարգացման հիմնական շարժիչ ուժերից մեկն էր: Համացանցի կառավարման տնտեսական տեսանկյունը կարևոր է այն բանով, որ կարող է լուսաբանել այն փաստաթղթի անվանումը, որը համացանցի կառավարման բարեփոխումների սկիզբը դրեց և հիմնադրեց ICANN՝ «Համաշխարհային էլեկտրոնային առևտրի հիմունքները» (1997): Այդ փաստաթղթում նշված է, որ «մասնավոր սեկտորը պետք է ղեկավարի» համացանցի կառավարման գործընթացը և այդ կառավարման հիմնական գործառույթը «էլեկտրոնային առևտրի համար կանխատեսելի, մինիմալիստական, հետևողական և պարզ իրավական միջավայրի» ապահովումն է: Այս սկզբունքները համացանցի կառավարման կարգի հիմքն են, որի կենտրոնում ICANN-ն է գտնվում:

Սահմանում

«Էլեկտրոնային առևտուր» հասկացության հստակ սահմանումն ունի բազում գործնական և իրավական հետևանքներ[1]: Եթե գործարքն էլեկտրոնային է ճանաչվում, ապա գործունեության այդ տեսակի կարգավորման հատուկ նորմեր են կիրառվում (մասնավորապես, հարկատրման և մաքսատուրքերի ոլորտում): ԱՄՆ կառավարության տեսակետի համաձայն, ավանդական առևտուրն էլեկտրոնայինից տարբերող հիմնական չափանիշն առցանց կարգով տրվող ապրանքներն ու ծառայությունները վաճառելու պարտավորությունն է: Սա նշանակում է, որ առցանց կնքված յուրաքանչյուր առևտրային գործարք, նույնիսկ եթե դրա իրականացումը ենթադրում է ապրանքի ֆիզիկական առաքում, դիտարկվում է որպես էլեկտրոնային: Օրինակ՝ Amazon.com կայքից գիրք ձեռք բերելը համարվում է էլեկտրոնային գործարք, չնայած, որ գիրքն առաքվում է սովորական փոստով: ԱՀԿ-ի տված

սահմանումն էականորեն արդեն իսկ «ապրանքների և ծառայությունների էլեկտրոնային արտադրություն, տարածում, գովազդում, առևտուր և առաքում է»: Համաշխարհային մաքսային կազմակերպությունը էլեկտրոնային առևտուրը սահմանում է հետևյալ կերպ. «գործարար գործարքներ իրականացնելու նպատակով՝ կազմակերպությունների անկախ համակարգչային տեղեկատվական համակարգերի միջև տվյալների փոխանակման համար, համակարգչային և հեռահաղորդակցային տեխնոլոգիաների կիրառման վրա հիմնված բիզնեսի վարման միջոց է»:

Էլեկտրոնային առևտրի տարբեր ձևեր գոյություն ունեն.

- business-to-consumer (B2C)՝ ֆիրման մասնավոր անձին վաճառում է ապրանք կամ ծառայություններ: Սա էլեկտրոնային առևտրի ամենատարածված տեսակն է (օրինակ՝ Amazon.com):

- business-to-business (B2B)՝ ֆիրմաների միջև իրականացվող առևտուր: Էլեկտրոնային առևտրի տնտեսապես առավել կարևոր տեսակն է, որը կազմում է էլեկտրոնային գործարքների ընդհանուր ծավալի 90 տոկոսը:

- business-to-government (B2G)՝ էկեկտրոնային պետգնումներ: Սա ամենակարևոր տեսակն է պետգնումների քաղաքականության տեսանկյունից:

- consumer-to-consumer (C2C)՝ մասնավոր անձինք այլ մասնավոր անձանց ապրանքներ են վաճառում և ծառայություններ մատուցում, օրինակ՝ էլեկտրոնային աճուրդները (ինչպիսին է՝ eBay):

Շատ երկրներ էլեկտրոնային առևտրի կարգավորման համար իրավական դաշտ են զարգացնում: Արդեն օրենքներ են ընդունվել էլեկտրոնային թվային ստորագրությունների, վեճերի լուծման, կիբեռհանցագործության, սպառողների իրավունքների պաշտպանության և հարկատվության վերաբերյալ: Միջազգային մակարդակով աճում է նաև էլեկտրոնային առևտրի հետ կապված նախաձեռնությունների ու կարգերի թիվը:

ԱՀԿ-ն և էլեկտրոնային առևտուրը

Միջազգային արդի առևտրում առանցքային խաղացողը՝ Առեւտրի համաշխարհային կազմակերպությունը կարգավորում է էլեկտրոնային առևտրի համար կարևոր շատ հարցեր, այդ թվում՝ հեռահաղորդակցությունների ազատականացումը, մտավոր սեփականության իրավունքների պաշտպանությունը և ՏՀՏ (Տեղեկատվական-հեռահաղորդակցային տեխնոլոգիաներ) զարգացման մի քանի տեսակետներ: Էլեկտրոնային առևտրի հետ անմիջական կապ ունեն ԱՀԿ գործունեության հետևյալ տեսակներն ու նախաձեռնությունները.

-Էլեկտրոնային գործարքների համար մաքսատուրքի վճարման ժամանակավոր դադարեցում, որը մտցվել է 1998 թ.: Դրանց համաձայն, համացանցում կատարվող բոլոր գործարքները ազատվեցին մաքսատուրքերից:

-Էլեկտրոնային առևտրի գծով ԱՀԿ աշխատանքային խմբի ստեղծումը, որի շրջանակներում շարունակվում է առևտրի այդ ձևին վերաբերող հարցերի շուրջ բանավեճը[2]:

-Վեճերի լուծման մեխանիզմ: Էլեկտրոնային առևտրին անմիջականորեն վերաբերող փայլուն օրինակ է «ԱՄՆ-ն ընդդեմ Անտիգուայի» գործը, որը կապված էր առցանց մոլի խաղերին[3]:

Էլեկտրոնային առևտրի հարցերը, թեև մինչև հիմա մտացել են ԱՀԿ գործունեության շրջագծում, այնուամենայնիվ այս ոլորտում շատ նախաձեռնություններ են եղել և նշվել են մի շարք առանցքային հարցեր: Ստորև դիտարկվում է երկու օրինակ:

Էլեկտրոնային առևտուրն, արդյոք, ապրանքների (GATT1 շրջանակներում կարգավորվող) կամ ծառայությունների (GATS2 շրջանակներում կարգավորվող) առևտուր է

Փոխվո՞ւմ է, արդյոք, օրինակ՝ աուդիոարդյունաբերության դասակարգումը (այսինքն՝ ապրանք է թե ծառայություն) կախված այն բանից, թե գնորդն ինչ միջոցով է այն ձեռք բերում՝ խտասկավառակով (նյութական ձևը), թե համացանցի (ոչ նյութական ձևը) միջոցով: Վերջին հաշվով, միևնույն երգը կարող է ունենալ տարբեր առևտրային կարգավիճակներ (և ենթակա լինի տարբեր հարկավճարների ու մաքսատուրքերի), կախված այն բանից, թե ինչ միջոցով է սպառողին առաքվում: Կարգավիճակի հիմնախնդիրը շատ կարևոր է, քանի որ ապրանքների առևտրի և ծառայությունների նկատմամբ տարբեր իրավակարգեր են կիրառվում:

Ինչ կապ պետք է լինի TRIPS-ի և Համացանցում մտավոր սեփականության իրավունքների պաշտպանության միջև

Քանի որ մտավոր սեփականության իրավունքի առևտրին առնչվող հայեցակետերի մասին պայմանագիրը (TRIPS), որ ստորագրվել էր ԱՀԿ շրջանակներում, մտավոր սեփականության իրավունքների ոլորտում կիրարկման ավելի հզոր մեխանիզմներ է ներկայացնում, քան ՄՍՀԿ պայմանագրերը, զարգացած երկրները փորձում էին ընդլայնել TRIPS կիրառման ոլորտը էլեկտրոնային առևտրի և համացանցի միջոցով, ընդ որում օգտագործելով երկու մոտեցում: Նախ՝ դիմելով «տեխնոլոգիական չեզոքության» սկզբունքին, նրանք նշում էին, որ ինչպես ԱՀԿ մյուս կանոնները, TRIPS նույնպես անհրաժեշտ է տարածել հեռահաղորդակցության, ներառյալ համացանցի միջոցով: Երկրորդ՝ զարգացած որոշ երկրներ պահանջեցին

ԱՀԿ, այսպես կոչված, թվային պայմանագրերի ավելի նեղ ինտեգրացում TRIPS համակարգում: Երկու հարցն էլ մտնում է բաց, դրանց կարևորությունը ԱՀԿ շրջանակներում հետագայում կաճի: Բանակցությունների ընթացիկ փուլում քիչ հավանական է, որ ԱՀԿ օրակարգում նշանակալի ուշադրություն կդարձվի էլեկտրոնային առևտրին: Այս ոլորտի վերաբերյալ գլոբալ պայմանագրերի բացակայությունը մասնակիորեն փոխհատուցվում է որոշ նախաձեռնություններով (դրանք վերաբերում են, օրինակ՝ պայմանագրերին և ստորագրություններին) և տարածաշրջանային տարբեր համաձայնագրերով, հիմնականում ԵՄ ու Ասիա-խաղաղօվկիանոսյան տարածաշրջանում:

1. Մաքսերի և առևտրի մասին գլխավոր համաձայնագիր (General Agreement on Tariff s and Trade)

2. Ծառայությունների առևտրի մասին գլխավոր համաձայնագիր (General Agreement on Trade in Services)

Էլեկտրոնային առևտրի ոլորտում միջազգային այլ նախաձեռնություններ

Էլեկտրոնային առևտրի բնագավառում ամենահաջող և մեծ աջակցություն ունեցող միջազգային նախաձեռնություններից մեկը էլեկտրոնային առևտրի մասին Տիպային օրենքն է, որը նախապատրաստել է ՄԱԿ-ի միջազգային առևտրի իրավունքի հանձնաժողովը (UNCITRAL): Այդ օրենքն, առաջին հերթին, նվիրված է էլեկտրոնային առևտրի ինտեգրման մեխանիզմներին և ավանդական առևտրային օրենսդրությանը: Այդ փաստաթուղթը շատ երկրներում դարձել է էլեկտրոնային առևտրին վերաբերող օրենսդրության հիմքը: Էլեկտրոնային առևտրի զարգացմանն ուղղված մեկ այլ նախաձեռնություն է Առևտրային ընթացակարգերի պարզեցման և e-business XML (ebXML) սահմանված չափորոշիչների էլեկտրոնային բիզնեսի (UN/CEFAT) վերաբերյալ ՄԱԿ-ի կենտրոնի մշակումը: XML լեզվի վրա հիմնված այդ չափորոշիչները մոտ ապագայում կարող են հիմք դառնալ էլեկտրոնային առևտրային փաստաթղթերի փոխանակման համար, դուրս մղելով ներկայում կիտառվող EDI (Electronic Data Interchange) չափորոշիչը: Եվրամիությունը նույնպես մի շարք միջոցներ է ձեռնարկել էլեկտրոնային առևտրի բնագավառում, հիմնականում կենտրոնանալով փոքր և միջին բիզնեսի հիմնախնդիրների վրա4: Էլեկտրոնային առևտրի հետ կապված շատ հարցեր, այդ թվում օգտատերերի իրավունքների պաշտպանությունը և էլեկտրոնային թվային ստորագրությունը շոշափվում են նաև ՏՀՀԿ գործունեության մեջ: Այդ կազմակերպությունը նպաստում է էլեկտրոնային առևտրի զարգացմանը և դրա հետ կապված հարցերի ուսումնասիրմանը՝ հանձնարարականների և հրահանգների հրապարակման ճանապարհով: Առևտրի և զարգացման մասին ՄԱԿ-ի համաժողովը (UNCTAD) ավելի ակտիվ է ուսումնասիրությունների և ներուժի զարգացման բնագավառում: Այն հիմնականում զբաղված է էլեկտրոնային առևտրի և զարգացման միջև

կապի հարցերով: Ամեն տարի UNCTAD-ը հրատարակում է «Էլեկտրոնային առևտուր և զարգացում» վերնագրով զեկուցումը, որն ընդգրկում է ընթացիկ իրավիճակի ամփոփումը և ապագայի համար հանձնարարականներ: Բիզնեսի ոլորտում ամենաակտիվ կազմակերպությունը Միջազգային առևտրի պալատն է, որը էլեկտրոնային առևտրի մասին թողարկում է մեծ թվով հանձնարարականներ և վերլուծական զեկույցներ, ինչպես նաև «Բիզնեսի գլոբալ երկխոսությունը էլեկտրոնային հասարակության վերաբերյալ» ընկերակցությունը, որն աջակցում է էլեկտրոնային առևտրի զարգացմանը ազգային և միջազգային մակարդակներում:

Տարածաշրջանային նախաձեռնություններ

2000 թ. Լիսաբոնում ԵՄ երկրների ղեկավարների, այսպես կոչված, Dot. Com գագաթաժողովում ԵՄ-ն ընդունել է էլեկտրոնային զարգացման ռազմավարությունը: Չնայած, որ էլեկտրոնային առևտրի առնչությամբ շեշտը դրվում էր մասնավոր և դեպի շուկան ուղղված նախաձեռնությունների վրա, սակայն ԵՄ շրջանակներում ընդունվեցին նաև որոշ շտկումներ՝ ուղղված պետական և հասարակական շահերի պաշտպանությանը (նպաստել համընդհանուր համացանցային հասանելիության ապահովմանը, պետական շահերին ուշադրություն դարձնող մրցութային քաղաքականություն, վնասակար նյութերի տարածման սահմանափակումը):

Համընդհանուր հասանելիության մասին մանրամասն բաժին 5-ում

ԵՄ-ն էլեկտրոնային առևտրի վերաբերյալ ընդունել է հրահանգ, ինչպես նաև մի շարք այլ փաստաթղթեր՝ էլեկտրոնային թվային ստորագրության, տվյալների պահպանության և էլեկտրոնային ֆինանսական գործարքների մասին: Ասիա-խաղաղօվկիանոսյան տարածաշրջանում էլեկտրոնային առևտրի ոլորտում փոխազդեցությունների կենտրոնը Ասիա-խաղաղօվկիանոսյան տնտեսական համագործակցության (ԱԽՏՀ՝ ATЭC) միջազգային կազմակերպությունն է: Էլեկտրոնային առևտրի ղեկավար խումբը, որ ստեղծվել է ԱԽՏՀ-ի շրջանակներում, ուսումնասիրում է էլեկտրոնային առևտրի հետ կապված տարբեր հարցեր, այդ թվում նաև սպառողների շահերի պաշտպանության, տվյալների պահպանության, փոստաղբի և կիբեռհանցագործության դեմ հակագործողությունների վերաբերյալ հարցեր: Վերջին և ամենանշանակալի օրենսդրական նախաձեռնությունը անթուղթ առևտրի զարգացման ուղղությամբ ԱԽՏՀ գործողությունների անհատական ծրագիրն է, որը նպատակաուղղված է 2010 թ. տարածաշրջանում ստեղծել միանգամայն առանց թղթաբանության փաստաթղթաշրջանառության առևտրի համակարգ:

Փոստաղբի և կիբեռանվտանգության մասին մանրամասն բաժին 2-ում

Սպառողների իրավունքների պաշտպանություն

Էլեկտրոնային առևտրի զարգացման հաջողության հիմնական պայմաններից մեկը սպառողների վստահությունն է: Գործունեության այս տեսակը համեմատաբար նոր է, այդ պատճառով սպառողները դեռևս չեն վստահում էլեկտրոնային առևտրին այնպես, ինչպես ավանդական առևտրին: Սպառողների իրավունքների պաշտպանությունը էլեկտրոնային առևտրի հանդեպ վստահության ամրապնդման իրավական կարևորագույն գործիք է: Էլեկտրոնային առևտրի կարգավորումը պետք է սպառողներին պաշտպանի տարբեր բնագավառներում՝ անբարեխիղճ գովազդից, անորակ ապրանքից և ծառայություններից, գողությունից կամ անձնական ֆինանսական տվյալների անօրինական փոխանցումից (օրինակ՝ տեղեկատվություն վճարման քարտերի մասին): Էլեկտրոնային առևտրի համար բնութագրական նոր առանձնահատկություն է դառնում միջազգային մակարդակում սպառողների իրավունքների պաշտպանության անհրաժեշտությունը, ինչը ավանդական առևտրի համար առաջնահերթություն չէ: Նախկինում սպառողները հազվադեպ էին զգում միջազգային պաշտպանության կարիք, քանի որ ապրանք էին ձեռքբերում և ծառայություններ ստանում իրենց երկրում: Էլեկտրոնային առևտրի զարգացման հետ պետության սահմաններից ավելի ու ավելի շատ են գործարքներ դուրս գալիս: Սպառողների իրավունքների պաշտպանության տեսանկյունից կարևոր հարց է իրավասության հիմնախնդիրը, որի համար երկու հիմնական մոտեցում գոյություն ունի: Առաջին մոտեցումն ավելի ձեռնտու է վաճառողների համար (առավելապես էլեկտրոնային առևտուր իրականացնող ընկերությունների համար) և հիմնվում է «ծագման երկրի» սկզբունքի կամ «նշանակված է վաճառող» սկզբունքի վրա: Այսպիսի սցենարի գոյության դեպքում էլեկտրոնային առևտրով զբաղվող ընկերություններն առավելություն են ունենում, քանի որ միշտ գործում են կանխատեսած և իրենց լավ ծանոթ իրավական միջավայրի շրջանակներում: Մեկ այլ մոտեցում, որն առաջին հերթին պաշտպանում է գնորդին, հիմնվում է «նշման երկրների» սկզբունքի վրա: Այստեղ ընկերությունների համար հիմնական բարդությունը դառնում է բազմաթիվ տարբեր իրավական համակարգերի հետ բախման հավանականությունը: Այս հիմնախնդրի լուծման համար առաջարկվող մեխանիզմներից մեկը սպառողների իրավունքների պաշտպանության ոլորտում տարբեր երկրների օրենսդրությունների ներդաշնակեցումն է, ինչն էլ իրավասության մասին հարցի հրատապությունը նվազեցնում է: Սպառողների իրավունքների պաշտպանության ոլորտում, ինչպես նաև էլեկտրոնային առևտրի բնագավառին առնչվող մյուս հարցերում, միջազգային ասպարեզում առաջատարի դեր է խաղում ՏՀԶԿ-ն: Այդ կազմակերպության շրջանակներում ընդունվել են՝ էլեկտրոնային առևտրի համատեքստում սպառողների իրավունքների պաշտպանության մասին հրահանգը (2000 թ.) և սպառողներին խարդախությունից ու խաբեբայական

գործողություններից առանց սահմանների պաշտպանելու մասին հրահանգը (2003 թ.): ՏՀԶԿ-ի մշակած հիմնական սկզբունքները փոխառել են ուրիշ գործարար ընկերակցություններ, ներառյալ Միջազգային առևտրի պալատը և Գործարար պրակտիկայի բարելավման գործակալությունների խորհուրդը: Սպառողների պաշտպանության բարձր մակարդակ է ապահովում ԵՄ-ը: Իրավասության հարցերը, մասնավորապես, լուծվում են ԵՄ երկրներում դատարանների որոշումների կատարման մասին Բրյուսելի պայմանագրի շրջանակներում, որը պահանջում է, որպեսզի սպառողներն իրենց իրավունքները պաշտպանելու համար միշտ կարողանան դիմել տեղական օրենսդրությանը և տեղական դատարաններին: Համաշխարհային մակարդակով միջազգային իրավական գործուն որևէ գործիք դեռևս չի ստեղծվել: Առավել կարևոր փաստաթղթերից մեկը Ապրանքների առուվաճառքի միջազգային պայմանագրերի մասին ՄԱԿ-ի պայմանագիրն է (1980 թ.), որը չի շոշափում սպառողական պայմանագրերի կնքման և սպառողների իրավունքների պաշտպանության հարցերը: Մի շարք մասնավոր ընկերակցություններ և ոչ կառավարական կազմակերպություններ նույնպես աշխատում են էլեկտրոնային գործարքների սպառողների իրավունքների պաշտպանության ոլորտում: Դրանց շարքին են պատկանում այնպիսի կազմակերպություններ, ինչպիսիք են՝ «Միջազգային սպառողներ», «Սպառողների տեխնոլոգիական նախագիծ», «Սպառողների պաշտպանության միջազգային ցանց» և «Ցանցի սպառողական մոնիտորինգ»: Էլեկտրոնային առևտրի հետագա զարգացումը կպահանջի կամ տարբեր երկրների օրենսդրությունների ներդաշնակեցում, կամ միջազգային նոր ռեժիմի ստեղծում՝ էլեկտրոնային առևտրի համատեքստում սպառողների իրավունքների պաշտպանության համար:

Հարկում

1831 թ., երբ Ֆարադեյը բացահայտել էր էլեկտրականության հիմնական սկզբունքները (էլեկտրամագնիսական դաշտի տեսությունը), թերահավատ մի քաղաքագետ նրան հարցրել է, թե ինչ օգուտ կարող է լինել էլեկտրականությունից: Ֆարադեյը պատասխանել է. «Պարոն, չգիտեմ, թե դրանից ինչ օգուտ կլինի, սակայն մի բանում համոզված եմ, որ կգա ժամանակ, երբ դուք դրանից հարկ կվերցնեք»5: Համացանցի կառավարման հարցում ծագած վեճն այն մասին, թե կիբեռտարածության վերաբերյալ հարցերն, արդյոք, պետք է դիտարկվեն որպես իրական աշխարհի երևույթներից տարբերվող, իր արտացոլումն է գտնում նաև հարկման հարցում6: ԱՄՆ-ն ի սկզբանե փորձում էր համացանցը հայտարարել հարկերից ազատ գոտի: 1998 թ. ԱՄՆ Կոնգրեսն ընդունել էր «Հարկերից ազատ լինելու մասին փաստաթուղթ», որը 2004 թ. դեկտեմբերին երեք տարով ևս երկարացվեց: 2007 թ. հոկտեմբերին այդ փաստաթղթի

ժամկետը երկարացվում է մինչև 2014 թ., չնայած վտանգ կար, որ դա կարող էր հանգեցնել բյուջե կատարվող մուտքերի նվազմանը7: ՏՀՉԿ-ն և ԵՄ-ն պնդում են հակառակ դիրքորոշումը, այն է՝ հարկման առումով համացանցի համար որևէ բացառություն չպետք է արվի: Օտտավայի ՏՀՉԿ սկզբունքներում նշվում է, որ ավանդական և «էլեկտրոնային» հարկումների միջև այնպիսի տարբերություններ չկան, որոնք կարող են պահանջել հատուկ կարգավորման ներմուծում: Այս սկզբունքի վրա է հիմնվում 2003 թ. ԵՄ-ում ընդունված օրենքը, որի համաձայն, էլեկտրոնային առևտրի այն ընկերությունները, որոնք ԵՄ տարածքում չեն գտնվում, Եվրամիության տարածքում ապրանքներ վաճառելու դեպքում պարտավոր են վճարել ավելացված արժեքի հարկ: Այդ օրենքի ընդունման օգտին հիմնական փաստարկն այն էր, որ ԵՄ տարածքից դուրս գտնվող ընկերությունները (հիմնականում ԱՄՆ-ում) եվրոպական ընկերությունների համեմատ, որոնք բոլոր գործարքների դեպքում, այդ թվում նաև էլեկտրոնայինին վրաբերող, պետք է ԱԱՀ վճարեն, առավելություններ ունեին:

Համացանցային առևտրի բնագավառում մեկ այլ հիմնախնդիր էր այն, թե որ պետության գանձարանին պետք է վճարվեր համապատասխան հարկերը: Այս հարցում ԱՄՆ և ԵՄ դիրքորոշումները նույնպես չէին համաձայնեցվում: ԱՄՆ-ն շահագրգռված էր, որ հարկերը վճարվեին ապրանքի «ծագման սկզբունքի» համապատասխան, քանի որ համացանցային առևտրով զբաղվող ընկերությունների մեծ մասը գրանցված են ԱՄՆ-ում: Դրան հակառակ, Օտտավայի սկզբունքներում կիրառվում է «նշման երկրներ» չափանիշը, ինչը համապատասխանում է ԵՄ շահերին, որտեղ էլեկտրոնային առևտրի տեսանկյունից, գնորդներն ավելի շատ են, քան վաճառողները:

Էլեկտրոնային թվայնացված ստորագրություններ

Ընդհանրացնելով, կարելի է ասել, որ թվայնացված ստորագրությունները գործիքներ են, որոնք հնարավորություն են տալիս մարդուն համացանցում բացահայտելու: Այդ պատճառով էլ դրանք կապված են համացանցի շատ տեսանկյունների հետ, ներառյալ իրավասությունը, կիբեռանվտանգությունը և էլեկտրոնային առևտուրը: Թվայնացված ստորագրությունների կիրառումը պետք է նպաստի համացանցում վստահելի հարաբերությունների հաստատմանը: Թվային ինքնությունը էլեկտրոնային առևտրի կարևոր բաղադրիչն է: Այն էլեկտրոնային պայմանագրերի միջոցով պետք է հեշտացնի էլեկտրոնային գործարքների կնքումը: Օրինակ՝ հեշտ չէ էլեկտրոնային փոստի միջոցով կամ վեբկայքում կնքված պայմանագրերի իսկության հարցը, չէ՞ որ շատ երկրներում օրենքը պահանջում է, որ յուրաքանչյուր պայմանագիր լինի «գրավոր» կամ «ստորագրված»: Ինչ է նշանակում դա համացանցի առնչությամբ: Նմանատիպ խնդիրներին բախվելով և էլեկտրոնային առևտրի համար բարենպաստ իրավական միջավայր ստեղծելու անհրաժեշտությունից

դրդված, շատ երկրների կառավարություններ սկսեցին օրենքներ ընդունել էլեկտրոնային թվային ստորագրությունների մասին (ԷԹՍ): Ինչ վերաբերում է ԷԹՍ-ին, ապա հիմնական բարդությունն այն է, որ կառավարությունները չեն փորձում լուծել գոյություն ունեցող հիմնախնդիրը (օրինակ՝ կիբեռհանցագործության կամ հեղինակային իրավունքի պաշտպանության դեմ հակագործողությունների դեպքում), այլ ստեղծում են մի նոր միջավայր, որն այդ բնագավառում փորձ չունի: Դա հանգեցրեց այն բանին, որ ի հայտ եկան տարբեր որոշումներ և էլեկտրոնային թվայնացված ստորագրություններին վերաբերող փաստաթղթերի հանդեպ համընդհանուր տարարժեքություն: Թվայնացված ստորագրությունների կարգավորման ոլորտում երեք գլխավոր մոտեցում կա8: Առաջին մոտեցումը «մինիմալիստականն» է, որի համաձայն, չի կարելի մերժել էլեկտրոնային ստորագրությունների գոյությունը այն հիմնավորմամբ, որ դրանք էլեկտրոնային տեսքով են: Այս տարբերակը նախատեսում է էլեկտրոնային ստորագրությունների կիրառման բազմաթիվ տարբերակներ և ընդունվել է իրավունքի այդպիսի համակարգի նախադեպ ունեցող երկրներում (ԱՄՆ, Կանադա, Ավստրալիա, Նոր Զելանդիա):

Երկրորդ մոտեցումը «մաքսիմալիստականն» է, որը որոշում է թվայնացված ստորագրությունների կառուցվածքն ու կիրառման ընթացակարգը, ներառյալ գաղտնագրերը և «բաց բանալիների» նույնացման կիրառումը: Այս մոտեցումը սովորաբար ենթադրում է հատուկ լիազոր մարմինների ստեղծում, որոնք կարող են արտոնագրել թվայնացված ստորագրության ապագա օգտատերերին: Այս մոտեցումը գերիշխում է եվրոպական այնպիսի երկրների օրենսդրություններում, ինչպիսիք են՝ Գերմանիան և Իտալիան:

Երրորդ մոտեցումը, որի օրինակը թվայնացված ստորագրությունների մասին ԵՄ հրահանգն է, զուգակցում է վերը նշված մոտեցումները9: Մինիմալիզմը երրորդ մոտեցման մեջ արտահայտվում է էլեկտրոնային տեսքով ստորագրությունների գոյությունը ճանաչող հատվածում: Մաքսիմալիստական մոտեցման տարրերն արտացոլվում են այն բանում, որ «կատարելագործված» թվայնացված ստորագրությունները իրավական տեսանկյունից ավելի մեծ կշիռ ունեն (օրինակ՝ դրանց օրինաչափությունը հեշտ է ապացուցել դատարանում): Թվայնացված ստորագրությունների մասին ԵՄ կանոնները հիմնախնդրի բազմակողմանիորեն լուծման օրինակ են: Այդ կարգադրությունները, թեև ընդունել են ԵՄ անդամ բոլոր պետությունները, այնուամենայնիվ, թվայնացված ստորագրությունների իրավական կարգավիճակի տարբերությունները պահպանվում են:

Միջազգային առևտրի իրավունքի մասին ՄԱԿ-ի հանձնաժողովը (UNCITRAL) 2001 թ. գլոբալ մակարդակով ընդունել է Էլեկտրոնային թվայնացված ստորագրությունների մասին տիպային օրենք, որն այդ ստորագրություններին սովորականներին հավասար կարգավիճակ է տալիս՝ պայմանով, որ դրանք պահպանեն որոշակի տեխնիկական պահանջներ: Միջազգային առևտրի պալատը մի փաստաթուղթ է կազմել, որն անվանել է

«Թվայնացմամբ հաստատված միջազգային առևտրային գործողությունների իրականացման ընդհանուր մեթոդները» (GUIDEC): Այդ փաստաթուղթը ընդգրկում է արտոնագրման դրական փորձի, կարգերի և հարցերի ամփոփումը10: Էլեկտրոնային թվայնացված ստորագրության հետ անմիջականորեն կապված են «բաց բանալու» (PKI) ենթակառուցվածքին առնչվող նախաձեռնությունները: Այդ ենթակառուցվածքի ստանդարտների ստեղծմամբ զբաղվում է երկու կազմակերպություն՝ ՀՄՄ-ն և IETF-ն:

Հարցեր

Մասնավոր կյանքի գաղտնիքի պահպանումն ու թվայնացված ստորագրությունները

Էլեկտրոնային թվայնացված ստորագրությունները ավելի մեծածավալ հիմնախնդրի՝ համացանցում գաղտնիության ու անձի ինքնության հավաստագրման միջև հավասարակշռության մի մասն է: ԵԹՍ-ն կարևոր տեխնոլոգիաներից ընդամենը մեկն է (բայց ոչ միակը), որ թույլ է տալիս համացանցում հավաստել օգտատիրոջ անձը11: Օրինակ՝ որոշ երկրներում, որտեղ ԵԹՍ-ին վերաբերող օրենսդրություն կամ ստանդարտներ ու ընթացակարգեր դեռևս մշակված չեն, առցանց գործողությունները խրախուսելու համար բանկերն անձի ինքնության հաստատումն իրականացնում են բջջային հեռախոսների օգնությամբ (SMS-ի միջոցով):

Իրավակիրառման ստանդարտների մանրամասն ստեղծման անհրաժեշտությունը

Զարգացած շատ երկրներ, թեև ԵԹՍ-ին առնչվող օրենսդրական փաստաթղթեր են ընդունել, սակայն այդ փաստաթղթերում հաճախ բացակայում են այդ օրենքների կիրառման ստանդարտների և ընթացակարգերի մանրամասն նկարագրությունը: Ուշադրության արժանացնելով այն, որ այս հիմնախնդիրը նոր է, շատ երկրներ սպասողական դիրք գրավեցին՝ փորձելով հասկանալ, թե ինչ ուղղությամբ են զարգանալու ստանդարտները: Ստանդարտացմանը վերաբերող նախաձեռնություններ են ի հայտ գալիս տարբեր մակարդակներում, ներառյալ միջազգային կազմակերպությունների (ՀՄՄ) և արհեստավարժ ընկերակցությունների (IETF) մակարդակներում:

Անհամատեղելիության վտանգը

Թվայնացված ստորագրությունների ոլորտում մոտեցումների և ստանդարտների բազմազանությունը կարող է հանգեցնել տարբեր ազգային համակարգերի անհամատեղելիության: Այդ հիմնախնդիրը «կտոր-կտոր» լուծելու մեթոդը կարող է սահմանափակել համաշխարհային մակարդակով էլեկտրոնային առևտրի զարգացումը: Անհրաժեշտ ներդաշնակությանը կարելի է հասնել տարածաշրջանային և համաշխարհային կազմակերպությունների օգնությամբ:

Էլեկտրոնային վճարումներ. համացանց-բանկային և էլեկտրոնային փողեր

Էլեկտրոնային վճարումների տարբեր սահմանումների համար միակ ընդհանուր բաղադրիչն այն է, որ ֆինանսական գործողությունները կատարվում են համացանցային միջավայրում՝ առցանց վճարման համակարգերն օգտագործելով: Էլեկտրոնային վճարումների համակարգի առկայությունն էլեկտրոնային առևտրի հաջող զարգացման նախադրյալն է: Էլեկտրոնային վճարումների բնագավառը պահանջում է «էլեկտրոնային փողեր» և «համացանց- բանկային» հասկացությունների սահմանազատում: Առցանց կարգով բանկային ծառայությունների տրամադրումը (համացանց-բանկային կամ էլեկտրոնային բանկային) ենթադրում է համացանցին միացած անձնական համակարգչի օգտագործումը՝ ավանդական բանկային գործողություններ իրականացնելու համար, ինչպիսիք են, օրինակ՝ դրամական փոխանցումներն ու վարկային քարտերով վճարումները: Նորը միայն գործողությունների իրականացման գործիքն է դառնում, իսկ գործողությունները մնում են նույնը: Համացանց-բանկային համակարգը նվազեցնում է գործարքների իրականացման համար կատարվող ծախսերը և օգտատերերին նոր հնարավորություններ է տրամադրում: Այսպես, օրինակ՝ հաճախորդի գործարքը, որը ավանդական ձևով կատարելիս բանկի համար արժենում է 1 դոլար, համացանց-բանկային ձևով կատարելիս արժե ընդամենը 0,02 դոլար12:

Կարգավորման տեսանկյունից, համացանց-բանկային ձևը նոր բարդություններ է ծնում պետական ֆինանսական մարմինների կողմից բանկերի արտոնագրմանը վերաբերող հարցում: Ինչպե՞ս արտոնագրել վիրտուալ բանկերը: Կարգավորման ոլորտին վերաբերող երկրորդ հարցը միջազգային մակարդակով օգտատերերի իրավունքների պաշտպանությունն է, ինչն արդեն լուսաբանվել է այս գրքում:

Համացանց- բանկային համակարգի համեմատ էլեկտրոնային փողերը նշանակալի նորամուծություն են: ԱՄՆ դաշնային պահուստային համակարգերը դրանք նշում են որպես էլեկտրոնային շրջանառության մեջ գտնվող փողեր: Էլեկտրոնային փողերը սովորաբար զուգորդվում են, այսպես կոչված, խելացի քարտերի (smart card) հետ, որ թողարկում են Mondex, Visa Cash և Cyber Cash ընկերությունները: Էլեկտրոնային բոլոր փողերն ունեն հետևյալ գծերը.

-պահվում են էլեկտրոնային տեսքով, ավելի հաճախ մագնիսական շերտով էլեկտրոնային քարտում կամ միկրոպրոցեսորային չիպում.

-շրջանառվում են էլեկտրոնային ձևով: Մեծ մասամբ օգտագործվում են վաճառող ֆիրմայի և գնորդի միջև կատարվող հաշվարկների համար,

սակայն հնարավոր է նաև ֆիզիկական անձանց միջև դրամական փոխանցումների իրականացում.

-Էլեկտրոնային փողերի օգտագործմամբ գործարքների իրականացումը բարդ համակարգ է, որը ներառում է էլեկտրոնային փողերի թողարկողին, ցանցային օպերատորներին և քլիրինգային գործողություններ իրականացնող բանկը:

Ներկայում էլեկտրոնային փողերի օգտագործումը գտնվում է զարգացման վաղ շրջանում: Էլեկտրոնային փողերը լայն տարածում չեն գտել, հիմնականում անվտանգության ու գաղտնիության պահպանման ոչ բավարար լինելու պատճառով: Էլեկտրոնային փողերի զարգացումը հնարավոր է երկու ուղղությամբ.

-աստիճանական, ինչը պահանջում է էլեկտրոնային գործարքների իրականացման միջոցների կատարելագործում, մասնավորապես, միկրովճարների արդյունավետ համակարգի զարգացում: Սակայն արդյունքում բոլոր գործարքների հիմքում գոյություն ունեցող բանկային և դրամական համակարգերն են լինելու.

-հեղափոխական, ինչը էլեկտրոնային փողերը երկրների կենտրոնական բանկերի վերահսկողությունից հանելու է: Միջազգային հաշվարկների բանկն արդեն ուշադրություն է դարձրել էլեկտրոնային փողերի զարգացման այնպիսի ռիսկերին, ինչպիսիք են կապիտալի և դրամական կուտակումների տեղաշարժերի վերահսկողության հնարավորությունների կրճատումը: Էլեկտրոնային փողերի թողարկումը, ըստ հայեցակարգի, կնշանակի երկրի կենտրոնական բանկի վերահսկողության բացակայությունը դրանց նկատմամբ: Այսպիսի մոտեցումը մասնավոր կազմակերպություններին հնարավորություն կտա սեփական փողը թողարկելու՝ էլեկտրոնային առևտրում այն օգտագործելու համար: Վերջին ժամանակներում տեղի ունեցած ֆինանսական ճգնաժամի և ֆինանսական համակարգի վերահսկողության իրեն վերապահված իրավունքը հետ վերադարձնելու կառավարությունների փորձերի համատեքստում քիչ հավանական է, որ էլեկտրոնային փողերի նկատմամբ իրականացվող փորձերը աջակցություն կստանան:

Հարցեր

1.Էլեկտրոնային փողերի և բանկային ծառայությունների հետագա առցանց տարածումը կարող է փոխել համաշխարհային բանկային համակարգը՝ սպառողներին տրամադրելով լրացուցիչ հնարավորություններ, միաժամանակ նվազեցնելով բանկային գործողությունների արժեքը: Տնտեսապես արդյունավետ բանկային առցանց ծառայությունները

լրջագույն մարտահրավեր են նետում «ապակուց և բետոնից» ավանդական բանկային մեթոդներին13: Հարկ է նշել, որ ավանդական ֆինանսական ինստիտուտներից շատերն արդեն ակտիվորեն կիրառում են համացանց-բանկային մեթոդը: 2002 թ. ԱՄՆ-ում կար ընդամենը 30 «վիրտուալ» բանկ: Այսօր արդեն դժվար է գտնել այնպիսի բանկ, որը էլեկտրոնային ծառայություններ չի տրամադրում:

2.Կիբեռանվտանգությունը էլեկտրոնային վճարումների լայնորեն տարածման ճանապարհին հիմնական բարդություններից մեկն է: Համացանցում ինչպե՞ս երաշխավորել ֆինանսական գործողությունների անվտանգությունը: Կիբեռանվտանգութճան մասին քննարկվում է այս գրքի մեկ այլ բաժնում: Այստեղ ընդամենն ընդգծվում է բանկերի և ֆինանսական այլ ինստիտուտների պատասխանատվությունն՝ առցանց գործողությունների անվտանգության համար: Այս տեսանկյունից կարևոր իրադարձություն է Enron, Arthur Andersen и WorldCom ընկերությունների մասնակցությամբ տեղի ունեցած ֆինանսական ամոթալի աղմուկին ի պատասխան ԱՄՆ Կոնգրեսի ընդունած, այսպես կոչված, Սարբանես-Օքսլիի փաստաթուղթը: Այդ օրենքն առցանց գործողությունների անվտանգության նկատմամբ բարձրացնում է ֆինանսական ինստիտուտների պատասխանատվությունը և ուժեղացնում է ֆինանսական վերահսկողությունը: Այն նաև անվտանգության համար պատասխանատվությունը կիսում է ֆինանսական ինստիտուտների և հաճախորդների միջև, ովքեր պետք է դրսևորեն ողջամտություն14:

3. Հարցումների համաձայն, վճարման միջոցների բացակայությունը (օրինակ՝ էլեկտրոնային քարտերի), իր նշանակությամբ երրորդ պատճառն է, որ ներունակ գնորդները չեն մասնակցում էլեկտրոնային առևտրին: Ներկայում էլեկտրոնային առևտուրը հիմնականում իրականացվում է վարկային քարտերի կիրառման միջոցով: Դա էլ էական խոչընդոտ է այն երկրների համար, որտեղ վարկային քարտերի շուկան զարգացած չէ: Այդ երկրների կառավարությունները պետք է անհրաժեշտ փոփոխություններ կատարեն իրենց օրենսդրություններում, որպեսզի արագացնեն վճարման քարտային համակարգերի ներմուծումը:

4. Էլեկտրոնային առևտրի զարգացմանը նպաստելու համար բոլոր երկրների կառավարությունները պետք է խրախուսեն անկանխիկ վճարման բոլոր ձևերը, ներառյալ վարկային քարտերն ու էլեկտրոնային փողերը: Էլեկտրոնային փողերի արագ ներմուծումը կպահանջի պետական կարգավորման լրացուցիչ միջոցառումներ: Էլեկտրոնային առևտրի ոլորտում Հոնկոնգը առաջինը համալիր օրենսդրություն ընդունեց, որից հետո 2000 թ. ԵՄ-ում ընդունվեց էլեկտրոնային փողերի մասին հրահանգ15: Կառավարությունները դժկամորեն են ներդնում էլեկտրոնային փողերը, քանի որ զգուշանում են երկրի կենտրոնական բանկի իշխանության

սահմանափակման հետ կապված ռիսկերից: Այդ մասին նախազգուշացնում են նաև շատ տնտեսագետներ: Այսպես, օրինակ՝ Դևիդ Սաքսթոնի խոսքերի համաձայն, «թվայնացված կանխիկ գումարը իրենից վտանգ է ներկայացնում երկրագնդի յուրաքանչյուր կառավարության համար, որը ցանկություն ունի կառավարելու իր ազգային արժույթը»: Կառավարությունները նույնպես անհանգստացած են այն հարցով, որ վճարման էլեկտրոնային միջոցները հնարավոր է օգտագործվեն փողերի լվացման համար:

5. Որոշ վերլուծաբանների կարծիքով, էլեկտրոնային առևտրի իսկապես մասշտաբային զարգացման հեռանկարները շատ բանով կապված են միկրովճարման արդյունավետ և հուսալի սպասարկում ներմուծելու հետ: Օրինակ՝ համացանցի օգտատերերը մինչ օրս դժկամորեն են օգտագործում վարկային քարտերը ոչ մեծ վճարումներ կատարելու համար (մի քանի դոլար կամ եվրո), որոնք գանձվում են որևէ հոդվածի կամ առցանց ուրիշ ծառայություններին հասանելիության թույլտվության համար: Էլեկտրոնային փողերի վրա հիմնված միկրովճարումների սխեման կարող է դառնալ այս հիմնախնդրի համար անհրաժեշտ լուծումը: Հետաքրքիր է նշել, որ համացանցի ստանդարտների բնագավառում առաջադեմ W3C կազմակերպությունը դադարեցրել է իր գործունեությունը էլեկտրոնային առևտրի և միկրովճարումների բնագավառում, ինչն այդ ուղղությամբ ստանդարտացման գործում համաշխարհային ջանքերի գործադրման մեջ մեկ քայլ հետ էր նշանակում16:

6. Հաշվի առնելով համացանցի բնույթը, միանգամայն հավանական է, որ էլեկտրոնային փողերը կդառնան համաշխարհային երևույթ, և դա առիթ կլինի այս հարցը միջազգային մակարդակով քննարկելու: Առցանց բանկային ծառայությունների տրամադրման բնագավառում գործող կազմակերպություններից մեկը Բազելի կոմիտեի բանկային էլեկտրոնային ծառայությունների տրամադրման խումբն է: Այն արդեն սկսել է զբաղվել անձի հավաստագրման, բարեհուսության, թափանցիկության, գաղտնիության, փողերի լվացման և բանկային գործունեության արտասահմանյան հսկողության ստուգման ստանդարտների հարցերով, որոնք էլեկտրոնային փողերի ներդրման տեսանկյունից կարևորագույն հարցեր են17:

7. Վերջերս Նյու Յորքի նահանգի գլխավոր դատախազի դիմումը Paypal համակարգին և Citibank բանկին, որով պահանջում էր հօգուտ համացանցային խաղատան վճարումներ չիրականացնել, անմիջականորեն իրար է միացնում էլեկտրոնային վճարումներն ու իրավակարգի ապահովումը18: Այն բանին, ինչին իրավապահ մարմինները չեն կարող հասնել իրավական մեխանիզմներով, կարող են հասնել էլեկտրոնային վճարումների վրա սահմանված վերահսկողությամբ:

Ծանոթագրություններ

1. Իրավական տեսակետից հստակ սահմանման նշանակությունը պարզորեն բացատրվում է ԵՄ-ի ինտերակտիվ էջում, որը նվիրված է էլեկտրոնային առևտրին. «Սովորաբար մենք խուսափում ենք էլեկտրոնային առևտրի սահմանումից, բացառությամբ այն ոչ հստակ սահմանումից, ըստ որի էլեկտրոնային առևտուրը կապված է էլեկտրոնային ձևով բիզնեսի վարման հետ: Սակայն իրավաբանական փաստաթղթերի համար անհրաժեշտ է իրավաբանական սահմանում...» (համացանցային հասցեն՝ http://ec.europa.eu/archives/ISPO/ecommerce/drecommerce/answers/000025.html):

2.ԱՀԿ-ի կայքի այս բաժինը նվիրված է էլեկտրոնային առևտրին՝ http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm:

3.Առցանց արգելված խաղերի կապակցությամբ «ԱՄՆ-ն ընդդեմ Անտիգուայի» գործի մասին լրացուցիչ տեղեկություններ կարելի է ստանալ համացանցային հետևյալ հասցեում՝ http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm:

4.Էլեկտրոնային առևտրի ոլորտում ԵՄ նախաձեռնությունների մասին լրացուցիչ տեղեկատվություն կարելի է ստանալ համացանցային հետևյալ հասցեում՝ http://europa.eu.int/information_society/eeurope/2002/action_plan/ecommerce/index_en.htm:

5. Maastricht Economic Research Institute on Innovation and Technology (MERIT) (համացանցային հասցեն՝ http://www.merit.unimaas.nl/cybertax/):

6.Համացանցի նկատմամբ կիրառվող հարկային քաղաքականության տարբեր տեսակետների քննարկումը տես՝ Arthur J. Cockfi eld, Transforming the Internet into a Taxable Forum: A Case

Study in E-Commerce Taxation, 85 MINN. L. REV. 1171, 1235-36 (2001); Edward

A. Morse, State Taxation of Internet Commerce: Something New under the Sun?, 30

CREIGHTON L. REV. 1113, 1124-27 (1997); W. Ray Williams, Th e Role of Caesar in

the Next Millennium? Taxation of E-Commerce: An Overview and Analysis, 27 WM.

MITCHELL L. REV. 1703, 1707 (2001):

7. «Making the 'Internet Tax Freedom Act' Permanent Could Lead to a Substantial Revenue

Loss for States and Localities» by Michael Mazerov (համացանցային հասցեն՝ http://www.cbpp.org/7-11-07sfp.htm):

8.Այս երեք մոտեցումների մասին մանրամասն բացատրությունը տես՝ Survey of Electronic and Digital Signature Initiatives provided by the Internet Law & Policy Forum (համացանցային հասցեն՝ http://www.ilpf.org/groups/survey.htm#IB):

9. Directive 1999/93/EC by the European Parliament and Council on 13 December 1999

on a Community Framework for Electronic Signatures.

10. GUIDEC (General Usage for International Digitally Ensured Commerce) by the International Chamber of Commerce (համացանցային հասցեն՝ http://www.iccwbo.org/home/guidec/guidec_one/guidec.asp).

11. Gavin Longmuir, «Privacy and Digital Authentication» (համացանցային հասցեն՝ http://caligula.anu.edu.au/~gavin/ResearchPaper.htm): Այս հոդվածը նվիրված է թվայնացման աշխարհում անձի հավաստագրման անձնական, հասարակական և պետական տեսակետներին:

12. Saleh M. Nsouli and Andrea Schaechter, «Challenges of the 'E-Banking Revolution'», Finance and Development, September 2002, Volume 39, Number 3, International Monetary Fund (համացանցային հասցեն՝ http://www.imf.org/external/pubs/ft /fandd/2002/09/nsouli.htm).

13. Հաջորդ հոդվածը նվիրված է համացանց-բանկային համակարգի ներմուծմանն ու բանկային ավանդական սպասարկման համեմատ դրա առավելություններին և թերություններին՝ http://www.bankrate.com/brm/olbstep2.asp:

14. Լրացուցիչ տեղեկատվություն կարելի է ստանալ հետևյալ հոդվածից՝ Edwin Jacobs, «Security as a Legal Obligation: About EU Legislation Related to Security and Sarbanes-Oxley in the European Union» (համացանցային հասցեն՝ http://www.arraydev.com/commerce/JIBC/2005-08/security.htm):

15. Directive 2000/46/EC of the European Parliament and Council of 18 September 2000 on the taking up, pursuit of, and prudential supervision of the business of electronic money institutions.

16.Միկրովճարումների դեմ բերվող փաստարկների մասին տես հետևյալ հոդվածում՝ «Th e Case against Micropayments» by Clay Shirky (համացանցային հասցեն՝ http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html:

17.Բազելի կոմիտեի խումբը աշխատում է Միջազգային հաշվարկների բանկին կից: Այն կանոնավոր կերպով հրապարակում է «Էլեկտրոնային փողերի և համացանցային ու բջջային վճարումների մասին նորությունների ամփոփումը» («Survey of Developments in Electronic Money and Internet

and Mobile Payments»).Տես՝ http://www.bis.org/publ/cpss62.pdf:

18. Տես՝ http://www.oag.state.ny.us/press/2002/aug/aug21a_02.html:

Բաժին 5

Զարգացման հարցեր

Զարգացման հարցեր

Տեխնոլոգիան չեզոք չի լինում: Մարդկային պատմությունը բազում օրինակներ ունի այն մասին, թե ինչպես են տեխնիկական նվաճումները որոշ մարդկանց, նույնիսկ միությունների ու երկրների տվել իշխանություն և հզորություն, մի կողմ թողնելով այլոց: Համացանցն, այս իմաստով, բացառություն չէ: Դրա տարածման շնորհիվ տեղի ունեցավ հարստությունների և իշխանության նշանակալի վերափոխումներ և՛ առանձին մարդկանց կյանքում, և՛ ողջ աշխարհով մեկ: Այն ազդեցությունը, որ համացանցն ու տեղեկատվական հեռահաղորդակցային տեխնոլոգիաներն ունեցան իշխանության բաշխման ու զարգացման վրա, առաջ է բերել բազմաթիվ հարցեր, օրինակ՝

-համացանցի- ՏՀՏ զարգացմամբ արագացված փոփոխություններն ինչ ազդեցություն են ունենալու Հյուսիսի և Հարավի միջև արդեն գոյություն ունեցող պառակտման վրա: Համացանց- ՏՀՏ-ն այդ ճեղքը կմեծացնի, թե՞ կնվազեցնի այն.

-զարգացող երկրները ե՞րբ և ինչպե՞ս կարող են հասնել զարգացած արդյունաբերական երկրների տեղեկատվական տեխնոլոգիաների մակարդակին: Այս և այլ հարցերին պատասխանելու համար անհրաժեշտ է համացանցի կառավարման զարգացման հետ կապված հիմնախնդրի վերլուծություն կատարել:

Ենթակառուցվածքի վերաբերյալ բաժին 3-ում

Համացանցի կառավարման համարյա յուրաքանչյուր տեսակետ ինչ-որ ձևով կապված է զարգացման հետ: Օրինակ՝ հեռահաղորդակցային ենթակառուցվածքի առկայությունը համացանց ներթափանցման իրավունքի տրամադրման հիմքն է, թվայնացված տեխնոլոգիաներում եղած խզումը հաղթահարելու համար առաջին նախապայմանը.

Տնտեսական խնդիրների վերաբերյալ բաժին 4-ում

-համացանցի ներթափանցման տնտեսական ընթացիկ մոդելը անհամաչափ ծանր բեռ է դնում զարգացող երկրների վրա, որոնք համացանցից օգտվելու համար պետք է վճարեն զարգացած երկրներում տեղակայված մայրուղիներ ներթափանցելու համար.

-փոստաղբը ավելի բացասական ազդեցություն է գործում զարգացող երկրների վրա, դրանց կապուղիների ցածր թողունակության և փոստաղբի դեմ պայքարի սահմանափակ հնարավորությունների պատճառով.

-մտավոր սեփականության իրավունքների ոլորտում միջազգային կարգավորումը անմիջականորեն ազդում է զարգացման վրա, քանի որ համացանցում

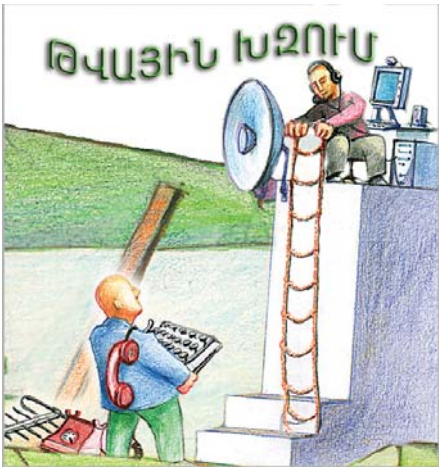
տեղադրված գիտելիքների և տեղեկատվության հասանելիության զարգացող երկրների իրավունքը սահմանափակ է:
WSIS-ի գործունեության համար զարգացման հարցերի կարևորությունը նշվում է շատ փաստաթղթերում. WSIS-ի վերաբերյալ ՄԱԿ-ի Գլխավոր վեհաժողովի բանաձևում ընդգծվում էր, որ գագաթաժողովը պետք է «նպաստի զագացմանը, հատկապես տեխնոլոգիաներին և դրանց փոխանցման հասանելիության իրավունքի առումով»: WSIS գործողությունների ծրագիրը և Ժնևի հռչակագիրը զարգացումը գլխավոր տեղում են դնում և դրա բանաձևը կապում են Հազարամյակների հռչակագրի հետ, ինչն անհրաժեշտ է համարում, որ. «զարգացման նպատակով բոլոր երկրներին հասանելի պիտի լինեն տեղեկատվությունը, գիտելիքներն ու հեռահաղորդակցային տեխնոլոգիաները»: Կապված լինելով «Հազարամյակների զարգացման նպատակների» հետ, WSIS-ն այդ բնագավառում կարևոր դեր է կատարում: Այս գլխում քննարկվում են զարգացման հետ կապված միայն հիմնական հարցերը՝ թվայնացված տեխնոլոգիաներում տեղի ունեցող խզումը և համընդհանուր հասանելիության ապահովումը: Հենց այդ հիմնախնդիրներն էլ հաճախ քննարկվում են զարգացման համատեքստում: Այստեղ վերլուծվում են նաև համացանցի և զարգացման վրա ազդող հիմնական գործոնները՝ ենթակառուցվածքը, ֆինանսական աջակցությունը, քաղաքական հարցերը և սոցմշակութային տեսակետները:

Հասարակության զարգացման վրա ինչպե՞ս են ազդում ՏՀՏ-երը

Տեղեկատվական տեխնոլոգիաների և զարգացման հետ կապված հիմնական հարցերը համառոտ շարադրված են The Economist ամսագրում տեղ գտած «Ընկնել ցանցի մե՞ջ» հոդվածում (2000 թ. սեպտեմբեր)[1]: Հոդվածը դեմ և կողմ փաստարկներ է բերում այն թեզիսի մասին, ըստ որի տեղեկատվական տեխնոլոգիաները զարգացման շարժիչ ուժն են:

ՏՀՏ-ն նպաստում է զարգացմանը	ՏՀՏ-ն չի նպաստում զարգացմանը
-«Ցանցային ազդեցություններն» օգնում են ՏՀՏ «պիոներներին» պահել գերիշխող դիրք, որի շնորհիվ ամերիկյան հսկա ընկերությունները էլեկտրոնային առևտրից դուրս են մղում զարգացող երկրների ոչ մեծ ֆիրմաներին: -Վաճառողի գերիշխող դիրքի կորուստը և գնորդի արժեքի բարձրացումը (համացանցում «այլ մատակարար միշտ կա՝ միայն պետք է մկնիկը շարժել») փաս է հասցնում ավելի աղքատ երկրներին, առաջին հերթին, զարգացող երկրների հումքային ապրանքներ արտադրողներին: -Զարգացած տնտեսություն ունեցող երկրներում «բարձր տեխնոլոգիական» գործողությունների գրավչությունը նվազեցնում է զարգացող երկրների հանդեպ ներդրողների հետաքրքրությունը:	-ՏՀՏ-ը նվազեցնում են աշխատանքի համար վճարվող ծախսերը, զարգացող երկրներում ներդրում կատարելն ավելի էժան է դառնում: -Ավելի վաղ գործող տեխնոլոգիաների համեմատ ՏՀՏ-ն արագ հաղթահարում է բոլոր սահմանները: Մյուս բոլոր տեխնոլոգիաները (օրինակ՝ երկաթուղիները և էլեկտրականությունը) զարգացող երկրներին հասնելու համար տասնամյակներ պահանջվեցին, այն դեպքում, երբ ՏՀՏ-ն շատ արագ է տարածվում: -Հնացած տեխնոլոգիաներից «առաջ ցատկելու» հնարավորությունը, անցումային փուլերի, ինչպիսիք են մետաղալարերն ու համանման հեռախոսային գործը, թողանցումն արագացնում է զարգացման թափը: -Արտադրության շատ ճյուղերում ֆիրմայի լավագույն չափը նվազեցնելու ՏՀՏ կարողությունը ավելի համապատասխանում է զարգացող երկրների պահանջներին:

Խզումը թվային տեխնոլոգիաներում



Թվայնացված տեխնոլոգիաներում տեղի ունեցող պառակտվածությունը («թվային խզում») կարելի է սահմանել որպես ջրբաժան նրանց միջև, ովքեր տեխնիկական, քաղաքական, սոցիալական կամ տնտեսական պատճառներից դրդված կարող են օգտագործել համացանցը-ՏՀՏ-ն, նաև նրանց միջև, ովքեր այդպիսի հնարավորություն չունեն: Թվայնացված տեխնոլոգիաների պառակտվածության ծավալների ու կարևորության վերաբերյալ տարբեր տեսակետներ գոյություն ունեն: «Թվային խզումը» (կամ ճեղքվածքները) տարբեր մակարդակներում են լինում՝ երկրի ներսում և երկրների միջև, քաղաքի և գյուղի բնակչության միջև, երիտասարդների և մեծահասակների միջև, ինչպես նաև կանանց և տղամարդկանց միջև:

«Թվային խզումները» մեկուսացված չեն լինում: Դրանք արտացոլում են կրթության և առողջապահության բնագավառում ստեղծված սոցիալ-տնտեսական անհավասարությունը, կախված են նյութական վիճակից, բնակատեղի որակից, աշխատանքի առկայությունից, մաքուր ջրից ու սնունդից: Ահա թե ինչ հետևության է հանգել «Մեծ ութնյակի» (DOT Force) թվային հնարավորությունների ուղղությամբ աշխատող նպատակային խումբը. «Ոչ մի հակասություն չկա «թվային խզման» և սոցիալական ու տնտեսական ավելի մեծ պառակտումների միջև, որոնք պետք է հաղթահարվեն զարգացման ընթացքում: «Թվային խզումը» հարկ է հասկանալ և հաղթահարել ավելի մեծ այս պառակտումների համատեքստում»[2]:

Մեծանո՞ւմ է, արդյոք, թվային խզումը

Համացանց-ՏՀՏ-ն զարգանում են ավելի արագ, քան մյուս բնագավառները (օրինակ՝ գյուղատնտեսությունը և առողջապահությունը), ու քանի որ, ի տարբերություն զարգացող երկրների, զարգացած երկրներում, որտեղ բոլոր հնարավորությունները կան ՏՀՏ-ի նվաճումների արդյունավետ օգտագործման համար, տպավորություն է ստեղծվում, թե «թվային խզումը» անընդհատ և մեծ արագությամբ մեծանում է:
Այս տեսակետը ներկայացված է բազմաթիվ հեղինակավոր աղբյուրներում, օրինակ՝ ՄԱԿ-ի Զարգացման ծրագրի մարդու զարգացման մասին զեկուցման մեջ և Աշխատանքի միջազգային կազմակերպության

զբաղվածության աստիճանի մասին զեկուցման մեջ: Հակառակ տեսակետի հիմքում այն կարծիքն է, որ թվային տեխնոլոգիաներում տեղի ունեցող խզումը գնահատող վիճակագրությունը հաճախ խաբուսիկ է և «թվային խզումը», փաստորեն, չի ավելանում: Այս դիրքորոշման համաձայն, համակարգիչների, վեբկայքերի քանակի և եղած հասանելիության կարողության նկատմամբ ավանդական ուշադրությունը պետք է փոխարինել զարգացող երկրներում ապրող մարդկանց՝ հասարակության վրա համացանց-ՏՀՏ-ի ազդեցության գնահատմամբ: Որպես օրինակ կարող են ծառայել թվային տեխնոլոգիաների բնագավառում Հնդկաստանի և Չինաստանի ձեռք բերած հաջողությունները:

Համընդհանուր հասանելիություն

«Թվային խզումից» բացի զարգացման վերաբերյալ բանավեճերում հաճախ հիշատակվող մեկ այլ հայեցակարգ է համընդհանուր հասանելիությունը, այսինքն՝ հասանելիություն բոլորի համար: Այս տեսակետը, թեև տեղեկատվական տեխնոլոգիաների նկատմամբ վարվող ցանկացած քաղաքականության հիմնաքարը պետք է լինի, սակայն գոյություն ունեն տարբեր կարծիքներ և տարբեր ըմբռնումներ՝համընդհանուր հասանելիության քաղաքականության մասշտաբների ու էության վերաբերյալ: Միջազգային բանաձևերի և հռչակագրերի ներածություններում այս հայեցակարգի հաճախակի հիշատակումը՝ քաղաքական և ֆինանսական անհրաժեշտ աջակցության բացակայության պայմաններում, այդ հասկացությունը վերածում է բավականին վերացական, որեւէ գործնական նշանակություն չունեցող մի սկզբունքի: Համընդհանուր հասանելիության հարցը միջազգային մակարդակով մտում է քաղաքական հարց, որը, վերջին հաշվով, կախված է այդ նպատակին հասնելու համար զարգացած երկրների ներդրումներ կատարելու պատրաստակամությունից: Ի տարբերություն միջազգային մակարդակի, որոշ երկրներում համընդհանուր հասանելիության հայեցակարգը տնտեսական և իրավական տեսանկյուններից մանրամասնորեն մշակվել է: Բոլոր քաղաքացիներին հեռահաղորդակցությունների հասանելիության տրամադրումը դրված էր հեռահաղորդակցությունների բնագավառում ԱՄՆ-ի վարած քաղաքականության հիմքում: Դրա արդյունքում ի հայտ եկավ քաղաքական ու ֆինանսական տարբեր մեխանիզմների լավ զարգացած համակարգ, որի նպատակը տարբեր շրջաններում և տարածաշրջանհերում, որտեղ կապը թանկ արժե, հասանելիության ֆինանսավորումն է: Դրամական օժանդակությունները տրամադրում են այն տարածաշրջանները, հիմնականում մեծ քաղաքները, որտեղ կապի գինը ցածր է: Համընդհանուր հասանելիության ապահովմանն ուղղված ԵՄ-ն նույնպես մի շարք միջոցներ է ձեռնարկել[3]:

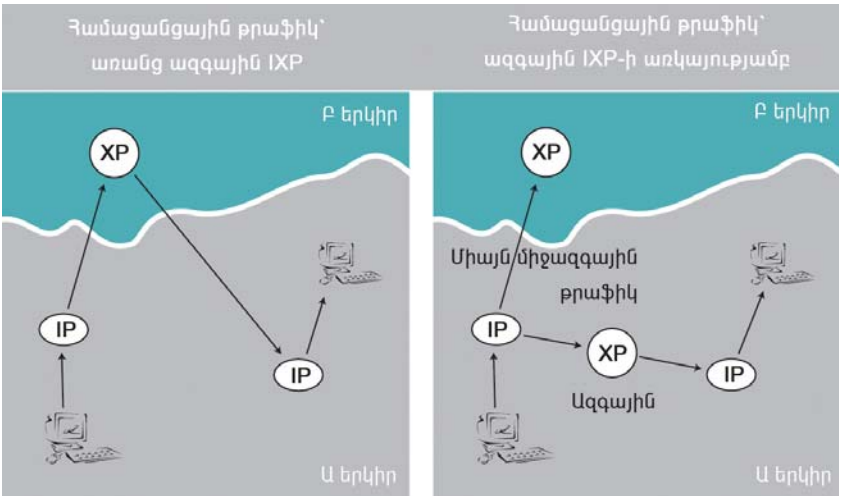
«Թվային խզումը» հաղթահարելու ռազմավարություն

Վերջին 50 տարիների ընթացքում քաղաքականության մեջ և ակադեմիական շրջանակներում գերիշխող զարգացման տեսությունը, որ կենտրոնացած է տեխնոլոգիայի վրա, հայտարարում է, որ զարգացումը կախված է տեխնոլոգիաների հասանելիությունից: Որքան շատ են տեխնոլոգիաները, այնքան մեծ է զարգացումը: Սակայն շատ երկրներում (հիմնականում նախկին սոցիալիստական պետություններում), այդ մոտեցումն իրեն չարդարացրեց: Պարզվեց, որ հասարակության զարգացումն ավելի բարդ գործընթաց է, իսկ տեխնոլոգիան թեև կարևոր, սակայն ոչ միակ նախապայմանն է այդ զարգացման: Մյուս տարրերը ներառում են չափորոշիչ շրջանակներ, ֆինանսական աջակցություն, մարդկային ռեսուրսների առկայություն, ինչպես նաև սոցմշակութային պայմաններ: Այս բոլոր բաղադրիչների առկայության դեպքում, նույնիսկ, անհրաժեշտ է իմանալ, թե ինչպես և երբ պետք է դրանք կիրառվեն, համապատասխանեցվեն և համագործակցեն:

Հեռահաղորդակցությունների և համացանցի ենթակառուցվածքների զարգացումը

Համաշխարհային ցանցի հասանելիությունն առանձին անհատների և կազմակերպությունների համար համացանցին ծանոթանալու, և արդյունքում՝ «թվային խզումը» հաղթահարելու անհրաժեշտ պայմանն է: Այդ հասանելիությունը ապահովելու և դրա որակը բարելավելու տարբեր միջոցներ գոյություն ունեն: Անլար կապի արագ աճը զարգացող շատ երկրների համար նոր հնարավորություններ է ստեղծում4: Intel ընկերության աշխատակից Պատրիկ Գելսինգերը զարգացող երկրների համար խելամիտ է համարում հրաժարումը հաղորդալարով իրականացվող կապից և «մատակարար-օգտատեր» հատվածում անլար կապի միջոցների կիրառումը, ինչպես նաև համազգային տեղեկատվական մայրուղիների համար օպտիկամանրաթելային ցանցի կիրառումը: Անլար հաղորդակցային կապը կարող է օգնել լուծելու վերերկրյա հեռահաղորդակցությունների ավանդական ենթակառուցվածքի զարգացման հիմնախնդիրը (ասիական և աֆրիկյան շատ երկրների հսկայական տարածությունների միջով մալուխներ անցկացնելու անհրաժեշտությունից ազատել): Այդ միջոցով կարելի է հաղթահարել «վերջին մղոնի» հիմնախնդիրը (տեղական կապուղու)՝ համացանցի արագ զարգացման ճանապարհին հիմնական խոչընդոտներից մեկը: Թվային խզման ավանդական ենթակառուցվածքային տեսակետները Հեռահաղորդակցության միջազգային միության (ՀՄՄ) ուշադրութան կենտրոնում են:

Ենթակառուցվածքի մասին մանրամասն բաժին 2-ում



Ֆինանսական աջակցություն

Զարգացող երկրները ֆինանսական աջակցություն են ստանում տարբեր ուղիներով, ներառյալ զարգացմանն աջակցող երկկողմանի և բազմակողմանի գործակալությունները (օրինակ՝ ՄԱԿ-ի զարգացման ծրագիրը կամ Համաշխարհային բանկը), ինչպես նաև զարգացման տարածաշրջանային նախաձեռնությունների և տարածաշրջանային բանկերի միջոցով: Հեռահաղորդակցային կապերի շուկայի ազատականացմամբ համապատասխան ենթակառուցվածքը ավելի հաճախ է ստեղծվում օտարերկրյա անմիջական ներդրումների շնորհիվ: Զարգացող երկրներից շատերը մշտական պայքար են մղում մասնավոր ներդրումներ ձեռք բերելու համար: Ներկայում արևմտյան հեռահաղորդակցային կապի ընկերությունների մեծ մասը գտնվում է միավորման փուլում, որի պատճառը մեծ պարտքերն են, որոնք առաջացել են 1990-ականներին մեծ չափերի հասնող ներդրումների արդյունքում: Նրանք, թեև դեռ պատրաստ չեն ներդրումներ կատարելու, սակայն հույս կա, որ մոտ ապագայում ընկերությունները դրամական ներդրումներ կկատարեն զարգացող երկրներում, քանի որ զարգացած երկրների շուկան գերհագեցած է 1990-ականների վերջին ստեղծված հզորություններով: Ֆինանսական տեսակետի կարևորությունը հատուկ ընդգծվել է տեղեկատվական հասարակության հարցերով համաշխարհային բարձր մակարդակի հանդիպման ընթացքում: Այդ հանդիպման որոշ մասնակիցներ հանդես եկան ՄԱԿ-ին կից թվային համերաշխության հիմնադրամ ստեղծելու առաջարկով, որի խնդիրներից էր լինելու հեռահաղորդակցային կապի ենթակառուցվածք ստեղծելու գործում աջակցել կարիքավոր երկրներին: Սակայն այդ առաջարկությունը զարգացած երկրների աջակցությանը չարժանացավ, քանի որ նրանց կարծիքով, անմիջական ներդրումները նախընտրելի են կենտրոնացված զարգացման հիմնադրամից: WSIS-ից հետո ժնևում ստեղծվեց թվային համերաշխության հիմնադրամ: Դա անկախ հիմնարկություն է, որին ողջ աշխարհում ֆինանսավորում են առավելապես քաղաքային եւ տեղական իշխանությունները:

Սոցմշակութային տեսակետներ

«Թվային խզման» սոցմշակութային բաղադրիչները ներառում են մի շարք հարցեր, ինչպիսիք են՝ գրագիտությունը, ՏՀՏ կիրառման հմտությունները, կրթությունը, լեզվաբանական բազմազանության պահպանումը: Զարգացող երկրների համար հիմնական բարդություններից մեկը «ուղեղների արտահոսքն է», որը ենթադրում է բարձրակարգ աշխատուժի արտահոսքը զարգացող երկրներից դեպի զարգացած երկրներ: Այդ պատճառով զարգացող երկրները կորցնում են միանգամից մի քանի ցուցանիշ: Դրանցից հիմնականը բարձրակարգ աշխատուժի արտահոսքն է: Զարգացող երկրները կորցնում են նաև դրամական այն միջոցները, որ ներդրվել են երկիրը լքող մասնագետների ուսման համար: Միանգամայն պարզ է, որ «ուղեղների արտահոսքը» շարունակվելու է, հատկապես հաշվի առնելով ԱՄՆ-ում, Գերմանիայում և այլ երկրներում արմատավորված ներգաղթի տարբեր ծրագրերը եւ աշխատանքի տեղավորման հեշտացված նախագծերը, որոնց նպատակը ՏՀՏ ոլորտի բարձրակարգ մասնագետներին գրավելն է: ՏՀՏ ոլորտի որոշ խնդիրների փոխանցումը (աութսորսինգը) զարգացող երկրներին կարող է դադարեցնել «ուղեղների հոսքը» կամ նույնիսկ նրանց հետ վերադարձնել: Դրա վառ օրինակ է ծրագրային ապահովման մշակմամբ զբաղվող կենտրոնների ստեղծումը Բանգալորեում և Հայդարաբադում (Հնդկաստան): ՄԱԿ-ը միջազգային մակարդակով հիմնադրել է թվային սփյուռքների ցանց՝ Աֆրիկայում զարգացման թափն արագացնելու համար՝ ՏՀՏ բնագավառում տեխնոլոգիական, գործնական ու մասնագիտական գիտելիքների և աֆրիկյան սփյուռքի ներուժը մոբիլիզացնելու միջոցով[5]:

Սոցմշակութային տեսակետների մասին մանրամասն բաժին 2-ում

Կարգավորումն ու քաղաքականությունը հեռահաղորդակցության ոլորտում

Հեռահաղորդակցությունների ոլորտում քաղաքականությունը սերտորեն կապված է «թվային խզումը» հաղթահարելու հետ: Նախ՝ և՛ մասնավոր, և՛ պետական ֆինանսական դոնորները պատրաստ չեն ներդրումներ կատարելու այնպիսի երկրներում, որտեղ չկա համացանցի զարգացման համար անհրաժեշտ ինստիտուցիոնալ ու իրավական միջավայր: Երկրորդ՝ ՏՀՏ ազգային հատվածների զարգացումը կախված է անհրաժեշտ իրավական շրջանակների ստեղծումից: Երրորդ՝ համացանցի հասանելիության շատ բարձր արժեքի պատճառներից մեկը հեռահաղորդակցության ազգային մենաշնորհների գոյությունն է:

ՏՀՏ զարգացման համար նպաստավոր պայմանների ստեղծումը բարդ խնդիր է, որը ենթադրում է՝ հեռահաղորդակցային կապերի շուկայի աստիճանաբար իրականացվող ապամենաշնորհացումը, համացանցի

վերաբերյալ օրենսդրության մշակում (հեղինակային իրավունքի, մասնավոր կյանքի իրավունքի, էլեկտրոնային առևտրի և այլ հարցերի վերաբերյալ), ինչպես նաև համընդհանուր հասանելիության ապահովումն առանց քաղաքական, կրոնական և այլ սահմանափակումների: Զարգացման վրա հեռահաղորդակցությունների շուկայի ազատականացման ազդեցության մասին քննարկումները տեղի են ունենում գերակշռող երկու տեսակետների շուրջ: Առաջինի կողմնակիցները պնդում են, որ ազատականացումը օգուտ չտվեց զարգացող երկրներին: Հեռահաղորդակցային մենաշնորհների կորստի հետ զարգացող երկրների կառավարությունները կորցրին իրենց բյուջեների համար շահույթի կարևոր աղբյուր: Բյուջեների կրճատումը հանգեցնում է հասարակական և տնտեսական կյանքի մյուս բնագավառներում տեղի ունեցող փոփոխությունների: Այս տեսակետի համաձայն, տանուլ են տվել զարգացող երկրների կառավարությունները, իսկ շահել են զարգացած երկրների հեռահաղորդակցային կապի ընկերությունները:

Օրենսդրական խնդիրների մասին մանրամասն բաժին 3-ում

Երկրորդ տեսակետը եզրակացնում է, որ հեռահաղորդակցությունների շուկայի բացումը հանգեցրեց մրցակցության ուժեղացման, որի արդյունքում բարձրացավ սպասարկման մակարդակը և նվազեցին գները: Ի վերջո կձևավորվի հեռահաղորդակցությունների արդյունավետ ու հասանելի մի հատված, ինչը հասարակության զարգացման համար անհրաժեշտ պայման է:

Ծանոթագրություն

1. «Falling through the Net?», Th e Economist, 21 September 2000.

2. Digital Opportunities for All: Meeting the Challenge. Report of the Digital Opportunity

Task Force (DOT Force) including a proposal for a Genoa Plan of Action. 11 May 2001 (համացանցային հասցեն՝http://www.g8italia.it/_en/docs/STUWX141.htm):

3. European Union. Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (համացանցային հասցեն՝ http://ec.europa.eu/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00510077.pdf):

4. Տես՝ United Nations. Press Release PI/1490. Development Potential of Wireless Internet Technology Explored at Headquarters Conference Resolution adopted by the General Assembly 56/183. World Summit on the Information Society. 27 June 2003 (համացանցային հասցեն՝ http://www.un.org/news/Press/docs/2003/pi1490.doc.htm;); Larry Press.

Wireless Internet Connectivity for Developing Nations// First Monday. Volume 8, number 9, September 2003 (համացանցային հասցեն՝ http://www.firstmonday.org/issues/issue8_9/press/):

5. Թվային սփյուռքների ցանցի մասին տեղեկատվությունը տես ՏՀՏ-ի վերաբերյալ ՄԱԿ-ի նպատակային խմբի կայքում՝ http://www.unicttaskforce.org/stakeholders/ddn.html:

Բաժին 6

Սոցմշակութային տեսակետներ

Սոցմշակութային տեսակետներ

Համացանցը նշանակալի ազդեցություն է գործել արդի հասարակության հասարակական ու մշակութային շերտի վրա: Դժվար է նշել հասարակական կյանքի մի բնագավառ, որի վրա այն ազդած չլինի: Համացանցը մեր կյանք է ներմուծում սոցիալական հեռահաղորդակցությունների նոր տեսակներ, ոչնչացնում է լեզվական արգելքները և ստեղծում է ստեղծագործական ինքնարտահայտման նոր ձևեր: Սրանք համացանցի ազդեցության ընդամենը մի քանի օրինակներ են: Այսօր համացանցն ավելի ու ավելի է դառնում սոցիալական, այլ ոչ թե միայն տեխնոլոգիական երևույթ: «Սոցմշակութային տեսակետներ» զամբյուղը ներառում է համացանցի կառավարման այնպիսի հարցեր, ինչպիսին է՝ նյութերի բովանդակության և բազմալեզվության նկատմամբ քաղաքականությունը: Այս հարցերը արտացոլում են ժամանակակից աշխարհի ազգային, կրոնական և մշակութային առավել աչքի ընկնող տարբերությունները:

Մարդու իրավունքները

Համացանցը մարդկությանը շփման ու փոխհարաբերությունների նոր ձևեր տվեց և, վերջին հաշվով, ազդեցություն գործեց մարդու իրավունքների ավանդական հասկացության վրա: Համացանցին առնչվող մարդու իրավունքների հիմնական ամբողջությունն ընդգրկում է մասնավոր կյանքի գաղտնիության, համոզմունքների արտահայտման ազատության, տեղեկատվություն ստանալու, կրթության իրավունքները, մշակութային և լեզվական բազմազանությունը պաշտպանող տարբեր իրավունքներ, ինչպես նաև փոքրամասնությունների իրավունքները: Զարմանալի չէ, որ մարդու իրավունքների հետ կապված հարցերը հաճախ են դարձել քննարկումների առարկա WSIS-ի և IGF-ի շրջանակներում: Մարդու իրավունքների հարցերը, թեև սովորաբար բացահայտորեն են քննարկվում, սակայն դրանք նույնպես ընդգրկված են այնպիսի «միջանցիկ» թեմաներում,

ինչպիսիք են՝ ցանցային չեզոքությունը (տեղեկատվության հասանելիության, արտահայտման ազատության, անվան գաղտնիության իրավունքներ), կիբեռանվտանգությունը (անվտանգության ապահովմանն ուղղված միջոցառումների ընթացքում մարդու իրավունքների պաշտպանություն), համացանցում տեղադրված նյութերի բովանդակության վերահսկողությունը և այլն: WSIS-ը կարևորել է մարդու իրավունքները, հատկապես զարգացման և համոզմունքների արտահայտման իրավունքները:

«Իրական իրավունքներ» և «կիբեռիրավունքներ»

Համացանցի կարգավորման համար գոյություն ունեցող օրենսդրության բավարար լինելու և նոր «կիբեռիրավունքի» պահանջարկի վերաբերյալ հայեցակարգային իրավական քննարկումներին զուգահեռ, բանավեճեր են տեղի ունենում այն մասին, թե արդյոք պետք է վերանայել մարդու իրավունքների ավանդական հայեցակարգերը՝ հաշվի առնելով համացանցի օգտագործումը: Քննարկվում են նաև մարդու «նոր» իրավունքները, ինչպիսին է՝ հեռահաղորդակցության համար իրավունքը:

Մարդու իրավունքներին և համացանցին վերաբերող նախաձեռնությունների ամփոփում

Ներկայում «կիբեռիրավունքների» ոլորտում առավել արդիական նախաձեռնությունը «Բիլը համացանցում իրավունքների մասին» (ԲՀԻ) աշխատությունն է, որին աջակցում են Իտալիան և քաղաքացիական հասարակության ներկայացուցիչները: «ԲՀԻ» շարժումը սկիզբ դրեց մի գործընթացի, որին աջակցում էր Դինամիկ կոալիցիան՝ համացանցային իրավունքների և թիվ 1 սկզբունքի համար, ու այսօր ընդգրկում է այնպիսի նախաձեռնություններ, ինչպիսին է «Համացանցային իրավունքի մոնիտորինգը»: «Բիլը համացանցում իրավունքների մասին» աշխատությունը քննարկվել է IGF բոլոր նստաշրջաններում: Ձգտելով սահմանել «կիբեռիրավունքները», Առաջադեմ հեռահաղորդակցությունների ընկերակցությունը նախապատրաստել է Համացանցային իրավունքների փաստաթղթի նախագիծ[1]: Մեկ այլ՝ ակադեմիական նախաձեռնություն է Ցանցային հեռահաղորդակցությունների ազատության մասին փաստաթուղթը, որը մշակվել է Տորոնտոյի համալսարանի իրավունքի ֆակուլտետում: 2008 թ. նոյեմբերին Google, Microsoft և մի շարք այլ համացանցային ընկերություններ կազմեցին գլոբալ ցանցային

Համացանցի հասանելիության իրավունք

Ֆինլանդիան առաջին պետությունն է աշխարհում, որ օրենսդրորեն երաշխավորում է համացանցի հասանելիությունը: 2010 թ. հուլիսից Ֆինլանդիայի բոլոր բնակիչները համացանցի 1Մգ լայնուղի հասանելիության իրավունք են ունենալու:

նախաձեռնություն, որի հիմնական նպատակը մարդու իրավունքների պաշտպանությունն է, հատկապես համոզմունքների ազատ արտահայտման և գաղտնիության իրավունքները: Այս նախաձեռնությունը առանձնահատուկ կարևորություն ունի, քանի որ հիմնական համացանցային ընկերությունների առևտրային գործունեությունը կարող է անմիջականորեն ազդել այն բանի վրա, թե ինչպես է իրականացվում մարդու իրավունքների պաշտպանությունը[2]:

Համացանցում մարդու իրավունքների պաշտպանության բնագավառում Եվրախորհրդի գործունեությունը

Համացանցում մարդու իրավունքների պաշտպանության բնագավառում հիմնական խաղացողներից մեկը Եվրախորհուրդն է, որը համաեվրոպական մակարդակով մարդու իրավունքների պաշտպանության հիմնական ինստիտուտն է: Եվրախորհրդի գլխավոր գործիքը Մարդու իրավունքների և հիմնական ազատությունների պաշտպանության մասին Եվրոպական պայմանագիրն է (1950)[3]: 2003 թ.-ից սկսած Եվրախորհուրդն ընդունել է մի քանի հռչակագրեր, որոնցում ընդգծվում է համացանցում մարդու իրավունքների կարևորությունը[4]: Այդ կազմակերպությունը նաև կիբեռհանցագործության մասին պայմանագրի ավանդապահն է՝ այդ բագավառում հիմնական գլոբալ գործիքը: Դա էլ Եվրախորհրդին դարձնում է արմատական ինստիտուտներից մեկը՝ ապագայում մարդու իրավունքների և կիբեռհանցագործության նկատառումների միջև անհրաժեշտ հավասարակշռություն գտնելու տեսակետից:

Կիբեռհանցագործության մասին մանրամասն բաժին 3-ում

Համոզմունքների ազատ արտահայտման և տեղեկատվություն որոնելու, ստանալու ու տարածելու իրավունք

Համացանցում մարդու իրավուվունքների ամենավիճելի ոլորտներից է համոզմունքների ազատ արտահայտման իրավունքը: Դա մարդու հիմնական իրավունքներից մեկն է, որը սովորաբար քննարկվում է գրաքննության ու համացանցում տեղադրվող նյութերի նկատմամբ վարվող քաղաքականության շրջանակներում: ՄԱԿ-ի Մարդու իրավունքների համընդհանուր հռչակագրում համոզմունքների ազատ արտահայտմանը (տես՝ 19) հակադրվում է այդ ազատությունը սահմանափակելու պետության իրավունքը՝ հանուն բարոյականության արդարացի պահանջների բավարարման, հասարակական կարգի և համընդհանուր բարեկեցության շահերի (տես՝ 29): Այդպիսով, հոդված 19-ի քննարկումն ու կյանքի կոչելը հարկ է դիտարկել այդ երկու պահանջների միջև անհրաժեշտ հավասարակշռության հասնելու համատեքստում: Այդպիսի երկիմաստ

իրավիճակը հնարավորություն է տալիս կարգերը և դրանց տարբեր կիրառումը մեկնաբանել ոչ միարժեքորեն: 19 և 29 հոդվածների միջև հակադրությունն «իրական» աշխարհում արտացոլվում է նաև համացանցում ճիշտ հավասարակշռություն գտնելու մասին բանավեճերում: Համոզմունքների ազատ արտահայտման իրավունքը գրավում է մարդու իրավունքների հետ առնչություն ունեցող ոչ պետական կազմակերպությունների առանձնահատուկ ուշադրությունը, այդ թվում նաև Amnesty International и Freedom House-ինը: Վերջերս Freedom House-ի կատարած ուսումնասիրությունները գնահատում են 6 տարածաշրջանների 15 երկրներում համացանցի և բջջային հեռախոսների օգտագործման ժամանակ հասարակ օգտատերերի ցուցաբերած ազատության մակարդակը: 2007-2008 թթ. կատարած ուսումնասիրությունը հաշվի է առնում մի շարք գործոններ, որոնք կարող են ազդել ազատ արտահայտման վրա, մասնավորապես, հեռահաղորդակցային ենթակառուցվածքների վիճակի, տեխնոլոգիաներին հասանելիության, համացանցային ծառայությունների մատակարարների նորմատիվային միջավայրի, գրաքննության և նյութերի բովանդակության վերահսկողության, իրավական միջավայրի նկատմամբ կառավարության սահմանափակումների, օգտատերերի և նյութեր ստեղծողների վրա անօրինական հարձակումների ու հետապնդման վրա: Նշված ինդիկատորները ընդգրկում են ոչ միայն կառավարության գործունեությունը, այլև յուրաքանչյուր երկրում նոր մեդիաների ակտիվությունն ու բազմազանությունը՝ անկախ դրանց կիրառումը սահմանափակելու կառավարության փորձերի կամ ի հեճուկս այդ փորձերի[5]:

Մարդու մյուս իրավունքները

Գաղտնիության իրավունքը քննարկվում է 144–149 էջերում: Սահմանափակ հնարավորություններով մարդկանց իրավունքները քննարկվում են 152–153 էջերում:

Համացանցում տեղադրված նյութերի բովանդակության նկատմամբ վարվող քաղաքականությունը

Համացանցի կառավարման սոցմշակութային տեսակետների շրջանակներում հիմնական հարցերից մեկը տեղեկատվական նյութերի բովանդակության (կոնտենտ) նկատմամբ վարվող քաղաքականությունն է, որը հաճախ քննարկվում է մարդու իրավունքների պաշտպանության (համոզմունքների ազատ արտահայտում և հեռահաղորդակցային կապ ունենալու իրավունք), կառավարության գործունեության (բովանդակության վերահսկողություն) և տեխնոլոգիաների (բովանդակությունը վերահսկելու գործիքներ) տեսանկյուններից: Համացանցի բովանդակության վերաբերյալ բանավեճերը սովորաբար հանգեցնում են երեք տեսակի նյութերի

քննարկման:
Առաջին խումբն ընդգրկում է անպիսի նյութեր, որոնց տարածումը վերահսկելու անհրաժեշտությունը կասկած չի առաջացնում: Դրանց շարքին են դասվում՝ մանկական պոռնոգրական, ցեղասպանությունն արդարացնող և ահաբեկչական գործողությունների կազմակերպման հետ կապված կամ դրանց մասին կոչ անող նյութերը, ինչպես նաև միջազգային իրավունքով արգելված այլ տեղեկատվություններ (ius cogens)[6]:
Երկրորդ խումբը ներառում է այնպիսի նյութեր, որոնք կարող են վիրավորական թվալ որոշակի երկրների, տարածաշրջանների կամ էթնիկ խմբերի համար՝ դրանց կրոնական կամ մշակութային առանձնահատկությունների պատճառով: Համաշխարհային առցանց հեռահաղորդակցային կապերը մարդկանց շատ խմբերի մշակութային և կրոնական արժեքներին մարտահրավեր են: Մերձավոր Արևելքում և ասիական երկրներում համացանցային նյութերի վերահսկողությունը պաշտոնապես բացատրում են որպես մշակութային առանձնահատուկ արժեքները պահպանելու անհրաժեշտություն: Սովորաբար դրա ներքո ենթադրվում է պոռնոգրական և արգելված խաղեր ներկայացնող կայքեր ներթափանցելու արգելքը[7]:
Երրորդ խումբը կազմված է համացանցում քաղաքական գրաքննության օրինակներից: 2007 թ. «Լրագրողներ առանց սահմանի» կազմակերպության ցուցակում թվարկվում էր համացանցում քաղաքական գրաքննություն իրականացնող 13 երկիր[8]:

Համացանցում տեղադրված նյութերի նկատմամբ ինչպե՞ս է իրականացվում քաղաքականությունը

Համացանցային նյութերի նկատմամբ իրականացվող քաղաքականության «ցանկը» ներառում է իրավական և տեխնիկական ստորև ներկայացվող հնարավորությունները, որոնք կիրառվում են տարբեր զուգադրություններով:

Բովանդակության զտումը կառավարության կողմից

Կառավարության կողմից նյութերի զտման ամենատարածված միջոցը վեբկայքերի «համացանցային ցանկն է», ուր քաղաքացիների ներթափանցումն արգելված է[9]: Վեբկայքը եթե ընդգրկված է այդպիսի ցանկում, ապա այն անհասանելի է: Տեխնիկական տեսանկյունից, զտումը հիմնականում իրականացվում է IP հասցեների շրջափակման միջոցով՝ մոտակա սպասարկուների և DNS-ին դիմելիս՝ վերանշանակման մակարդակով[10]:

Նյութերի զտումն իրականացվում է շատ երկրներում: Բացի այն երկրներից, որոնք զուգակցվում են այդ պրակտիկայով, օրինակ՝ Չինաստանը, Սաուդյան Արաբիան և Սինգապուրը, այն տարածում է գտնում նաև այլ երկրներում: Օրինակ՝ Ավստրալիայում գործում է զտման համակարգ՝ երկրի ներսում առանձին էջերի համար (սակայն ոչ արտասահմանյան կայքերի համար)[11]:

Վարկանիշի և զտման մասնավոր համակարգերը

Պետական տարբեր տեսակի խոչընդոտների ի հայտ գալով (զտման համակարգ) համացանցի մասնատման վտանգին բախվելով W3C-ը և նմանատիպ այլ ինստիտուտները «աշխատեցին առաջ անցնել»՝ առաջարկելով օգտագործել հիմնական օգտատերերի կողմից վերահսկվող վարկանիշների և զտման համակարգերը[12]: Համակարգերում զտման այդպիսի մեխանիզմները տեղադրվում են համացանցային զննարկիչներում: Որոշակի կայքում որոշ նյութերի հասանելիությունը նշվում է հատուկ նշանով: Այդպիսի զտման կիրառումը հատկապես տարածված է «երեխաների համար» կայքերում:

Երկրատեղորոշման ծրագրային ապահովում

Համացանցի նյութերի հետ կապված մեկ այլ տեխնիկական լուծում է երկրատեղորոշման ծրագրային ապահովումը, որը զտում է օգտատերերի հասանելիությունը որոշակի նյութերին՝ ըստ նրանց գտնվելու աշխարհագրական վայրի: Այս տեսակետից կարևոր նախադեպ էր Yahoo!-ի գործը, քանի որ դրանով զբաղվող փորձագետների խումբը, որի կազմում էր Վինտ Սերֆը, հայտարարել է, որ գործերի 70-90 տոկոսում Yahoo!-ն հնարավորություն ուներ որոշելու, թե կայքի նացիստական հիշարժան նյութեր պարունակող բաժին մուտք գործելու փորձ կատարող օգտատերն արդյոք Ֆրանսիայում է գտնվում[13]: Տեխնիկական այսպիսի գնահատականը օգնեց դատարանին վերջնական որոշում ընդունել. Yahoo!-ից պահանջեցին զտել Ֆրանսիայից հասանելիությունը դեպի նացիստական նյութեր պարունակող պորտալ:

Իրավական խնդիրների մասին
մանրամասն
բաժին 3-ում

Երկրատեղորոշման ծրագրային ապահովմամբ զբաղվող ընկերությունները հայտարարում են, որ կարող են անսխալ որոշել երկիրը, իսկ քաղաքը՝ դեպքերի մոտ 85 տոկոսում, հատկապես եթե մեծ քաղաք է14: IPv6 արձանագրության տարածման հետ միասին, որում յուրաքանչյուր սարք համացանցում ունի եզակի հասցե, երկրատեղորոշումը դառնում է ավելի հեշտ:

Որոնման համակարգերի օգնությամբ նյութերի վերահսկողությունը

Համացանցում տեղադրված նյութերի և օգտատերեի միջև «կամրջակ է» որոնման համակարգը: Մամուլում հայտնված որոնման համակարգերի օգնությամբ նյութերի վերահսկողության առաջին օրինակներից են Չինաստանի իշխանությունների գործողությունները Google որոնման համակարգի նկատմամբ: Եթե օգտատերն արգելված բառեր էր մուտքագրում որոնման համակարգում, ապա համակարգիչը մի քանի րոպե կորցնում էր համացանցի հետ կապը[15]: Չինաստանի տեղեկատվության նախարարության ներկայացուցիչը հայտարարել էր. «Միանգամայն նորմալ է այն, որ երբեմն անհնար է լինում ներթափանցել որոշ կայքեր:

Նախարարությունը չի ստացել որևէ տեղեկատվություն այն մասին, որ Google-ը ուղեկապվում է»[16]: Տեղական օրենքներին ընտելանալու համար Google-ում որոշում են սահմանափակել իրենց տարածաշրջանային վեբկայքերի որոշ նյութերին հասանելիությունը: Օրինակ՝ Google-ի գերմանական կամ ֆրանսիական տարբերակներում անհնար է գտնել նացիստական նյութեր պարունակող վեբկայքեր: Որոշակի առումով այդ ինքնագրաքննությունը կատարվում է հավանական դատական հայցերից խուսափելու համար[17]:

Վեբ 2.0 կանչ. օգտատերերը որպես հեղինակներ

Վեբ 2.0 հարթակների՝ բլոգների, ֆորումների, փաստաթղթերի փոխանակման և վիրտուալ աշխարհների ծառայությունների զարգացման հետ միասին օգտատերերի և բովանդակությունը (կոնտենտ) ստեղծողների միջև տարբերությունը վերանում է: Համացանցի օգտատերերը կարող են ինքնուրույն ստեղծել նյութերի մեծ մասը՝ բլոգների հաղորդագրություն, YouTube-ում տեսանյութեր տեղադրել, ֆոտոպատկերասրահ: «Անհամապատասխան» կայքերի ի հայտ գալը, զտումը և մակնշումը ավելի ու ավելի բարդանում է: Չնայած ավտոմատ զտման, ավտոմատ ճանաչման տեխնոլոգիաների գոյությանը, պատկերների և տեսանյութերի զտման ու կատեգորիաների սահմանումը դեռևս անհասանելի են: Վերանայել և բոլոր նյութերը ձեռքով նշել անհնար է, որոշ տվյալների համաձայն, 2006 թ. կեսերին YouTube-ում տեղադրվել է ավելի քան 6 մլն տեսահոլովակ, իսկ դրանք դիտելու համար օգտատերերի կորցրած ընդհանուր ժամանակը կազմել է ավելի քան 9000 տարի[18]: Հարավոր լուծումներից մեկը, որ կիրառվել է Մարոկոյում, Պակիստանում, Թուրքիայում և Թունիսում, երկրում YouTube ներթափանցման լիարժեք շրջափակումն է: Սակայն այդպիսի «մաքսիմալիստական» մոտեցման արդյունքը դառնում է առարկություն չառաջացնող,այդ թվում նաև կրթական նյութերի անհասանելիությունը:

Համապատասխան իրավական բազայի ստեղծման անհրաժեշտությունը

Համացանցի նյութերի առնչությամբ իրավական վակուումը կառավարություններին հնարավորություն է տալիս նյութերը ուղեկապել ըստ իրենց հայեցողության: Քանի որ բովանդակության (կոնտենտի) կարգավորումը յուրաքանչյուր հասարակության համար կարևորագույն հարց է, ապա այդ բնագավառում գոյություն ունի իրավական գործիքների մշակման կենսական անհրաժեշտություն: Համացանցի նկատմամբ պետական քաղաքականությունը կարող է ապահովել մարդու իրավունքների ամենալավ պաշտպանությունը և երբեմն պարզաբանել համացանցի ծառայությունների մատակարարների, իրավապահ մարմինների և այլ անձանց երկիմաստ դերը: Վերջին տարիներին շատ երկրներում համացանցում տեղադրվող նյութերի նկատմամբ վարվող քաղքականությունը սահմանող օրենսդրություն է ընդունվել:

Միջազգային նախաձեռնություններ

Միջազգային մակարդակով հիմնական նախաձեռնությունները բխում են եվրոպական երկրներից, որոնք ունեն անհանդուրժողականության տարբեր դրսևորումներին, ներառյալ ռասիզմն ու հրեատեցությունը, վերաբերող հզոր իրավական բազա: Եվրոպական տարածաշրջանային ինստիտուտներն այդ կանոնները փորձում էին մտցնել կիբեռտարածության մեջ: Համացանցում տեղադրվող նյութերի բովանդակության վերաբերյալ հարցերի կարգավորման հիմնական իրավական գործիքը ԵԽ կիբեռհանցագործության վերաբերյալ պայմանագրին կից լրացուցիչ արձանագրությունն է: Համացանցային նյութերի վերահսկողության ոլորտում Եվրամիության առաջին նախաձեռնությունը դարձավ «Եվրահանձնաժողովի հանձնարարականներն ընդդեմ համացանցում ռասիզմի դրսևորումների» փաստաթղթի ընդունումը: Այդ ուղղությամբ որպես գործնական քայլ մշակվել է անվտանգ համացանցի ստեղծման գործողությունների ծրագիրը, որը ներառում է հետևյալ հիմնական կետերը.

-Եվրոպայում միասնական «թեժ գծի» ստեղծումը, որի միջոցով կարելի է հաղորդել ի հայտ եկած անօրինական նյութերի մասին.

-ինքնակարգավորման խրախուսում.

-բովանդակության, զտման համակարգերի վարկանիշի ստեղծում, այդ թվում նաև չափանիշների հիման վրա.

-ծրագրային ապահովման և ծառայությունների մշակում.

-համացանցի անվտանգ օգտագործման մասին հանրամատչելի գիտելիքներ[19]:

Եվրոպայի անվտանգության և համագործակցության կազմակերպությունը (ԵԱՀԿ) այդ ոլորտում նույնպես ակտիվ գործունեություն է վարում: 2003-ից այն մի շարք հանդիպումներ ու համաժողովներ է կազմակերպել՝ նվիրված համոզմունքների ազատ արտահայտմանն ու համացանցի օգտագործման հավանական բացասական տարբերակներին (օրինակ՝ ռասիզմ, այլատյացություն և հրեատյացություն քարոզելու նպատակով):

Հարցեր

Համացանցային նյութերի վերահսկողությունը և համոզմունքների ազատ արտահայտում

Կոնտենտի վերահսկողության ոլորտում մեդալի հակառակ կողմը համոզմունքների ազատ արտահայտման սահմանափակումն է: Սա հատկապես կարևոր է ԱՄՆ–ում, որտեղ Սահմանադրության մեջ կատարված

առաջին ուղղումը երաշխավորում է ազատ արտահայտման իրավունքն ամենալայն իմաստով, ներառյալ ազգայնամոլական նյութերի և դրանց նման տեղեկատվության հրապարակման իրավունքը:
Համոզմունքների ազատ արտահայտումը շատ բաներում որոշում է ԱՄՆ-ի դիրքորոշումը համացանցի կառավարման հարցի վերաբերյալ միջազգային բանավեճում: Այսպես, թեև ԱՄՆ-ն ստորագրել է կիբեռհանցագործության մասին պայմանագիրը, սակայն չի կարող ստորագրել դրան կից լրացուցիչ արձանագրությունը, որը վերաբերում է անհանդուրժելի արտահայտություններին և նյութերը վերահսկելուն: Համոզմունքների ազատ արտահայտումը քննարկվել է նաև Yahoo!-ի գործի համատեքստում: Միջազգային բանակցությունների ընթացքում ԱՄՆ-ն փոխզիջման չի գնա, ինչը կարող է կասկածի ենթարկել Սահմանադրության առաջին ուղղմամբ պաշտպանվող համոզմունքների ազատ արտահայտման հարցը:

«Ցանցից դուրս անօրինականը՝ անօրինական է առցանցում»

Համացանցային նյութերի բովանդակության վերաբերյալ բանավեճը, այսպես թե այնպես շոշափում է իրական աշխարհի ու «կիբեռաշխարհի» միջև տարբերությունը: Գոյություն ունեցող օրենքները, որոնք կանոնակարգում են տարածվող նյութերի բովանդակությունը, կարող են կիրառվել նաև համացանցում: Այս փաստը հաճախ ընդգծվում է Եվրոպայում: Ռասիզմի և այլատյացության դեմ պայքարի ԵՄ խորհրդի շրջանակային որոշման մեջ բացահայտորեն նշվում է. «Այն, ինչը անօրինական է ցանցից դուրս՝ պետք է անօրինական մնա նաև առցանցում»: Համացանցի կառավարման հանդեպ «կիբեռմոտեցման» կողմնակիցների առաջ քաշած փաստարկներից մեկն այն է, որ քանակն ազդում է որակի վրա (հեռահաղորդակցային կապի ուժգնությունը, հաղորդագրությունների քանակը): Այս տեսակետի համաձայն, անհանդուրժելի արտահայտությունների հիմնախնդիրն այն չէ, որ բացակայում են համապատասխան կանոնավորող փաստաթղթերը, այլ այն, որ համացանցում տեղեկատվության փոխանակման ծավալները և դրանց փոխանակումը իրավական խնդիրներին նոր հատկանիշներ են տալիս: Ավելի ու ավելի շատ մարդկանց է հասանելի հակաօրինական նյութերը, այդ պատճառով էլ գոյություն ունեցող կարգի պահպանման ապահովումը բարդ է: Հետևաբար, իրավական տեսակետից համացանցի եզակիությունը ոչ թե օրենքներն են, այլ դրանց կիրառումն ու պահպանումն է:

Համացանցային նյութերը վերահսկելու արդյունավետությունը

Համացանցում տեղադրվող նյութերի վերաբերյալ քաղաքականությունը քննարկելիս, հիմնական փաստարկներից մեկը համաշխարհային ցանցի ապակենտրոնացված բնույթն է լինում, որը օգտատերերին հնարավորություն է տալիս գրաքննությունը շրջանցելու: Համացանցն ընդգրկում է տարբեր որոշումներ, որոնք թույլ են տալիս արդյունավետ վերահսկողություն իրականացնել, սակայն տեխնիկական տեսակետից դրանք կարելի է շրջանցել: Այն երկրներում, որտեղ համացանցային

նյութերի վերահսկողությունը պետական մակարդակով է կատարվում, տեխնիկապես առաջադեմ օգտատերերը կարողացան գտնել շրջանցման ուղիներ: Այնուամենայնիվ, կոնտենտի վերահսկողությունն ուղղված է ոչ թե օգտատերերի այդ փոքր խմբի դեմ, այլ բնակչության ավելի լայն շերտերի: Ինչպես գրել է Ռ. Գ. Կոուզը. «Կարգավորումը բավականաչափ արդյունավետ լինելու համար չպետք է բացարձակապես արդյունավետ լինի»:

Նյութերի նկատմամբ վարվող քաղաքականության համար ո՞վ է պատասխանատու

Նախ՝ Համացանցում տեղադրվող նյութերի բովանդակությունը կարգավորում են կառավարությունները: Նրանք որոշում են, թե ինչն է վերահսկողության ենթակա և ինչպես պետք է իրականացվի վերահսկողությունը: Համացանցային ծառայությունների մատակարարները ՝ որպես համացանցում հիմնական «միջնորդներ», պատասխանատու են կոնտենտի զտումն իրականացնելու համար, որն իրագործում են կամ կառավարության հրահանգի համաձայն, կամ ինքնակարգավորման հիման վրա (ծայրահեղ դեպքում, այնպիսի նյութերի առնչությամբ, ինչպիսիք են մանկական պոռնոգրաֆիկ նյութերը): Օգտատերերի որոշ խմբեր, օրինակ՝ ծնողները ձգտում են ուժեղացնել իրենց հսկողությունը, որպեսզի վտանգից հեռու պահեն իրենց երեխաներին: Երեխաների համար անթույլատրելի վեբկայքերը զտելու հարցում ծնողներին օգնելու համար ստեղծվել են վարկանիշային տարբեր համակարգեր: Համացանցային զննարկիչների նոր տարբերակները, սովորաբար, ներառում են զտման տարբեր հնարավորություններ: Համացանցում տեղադրված նյութերի վերահսկողությունը նույնպես իրականացնում են մասնավոր ընկերություններն ու համալսարանները: Որոշ դեպքերում բովանդակությունը վերահսկվում է ծրագրային ապահովման փաթեթի միջոցով: Օրինակ՝ սայենտաբանների շարժման անդամների մեջ տարածվել էր ՊՕ Scienositter փաթեթը, որն ուղեկապում էր սաենտաբանությունը քննադատող կայքեր ներթափանցումը[20]:

Մասնավոր կյանքի գաղտնիքը և տվյալների պահպանումը[21]

Մասնավոր կյանքի գաղտնիքի ու տվյալների պահպանումը միմյանց միջև սերտորեն կապված համացանցի կառավարման տեսակետներ են: Տվյալների պահպանումն իրավական մեխանիզմ է, որն ապահովում է մասնավոր կյանքի գաղտնիքի պահպանությունը: Ի՞նչ է «մասնավոր կյանքը» (privacy): Սովորաբար այն սահմանում են որպես յուրաքանչյուր քաղաքացու՝ անձնական տեղեկատվությունը վերահսկելու և դրա վերաբերյալ որոշումներ կայացնելու իրավունքը (բացել կամ չբացել այդ տեղեկատվությունը): Մասնավոր կյանքի իրավունքը յուրաքանչյուր մարդու անբակտելի

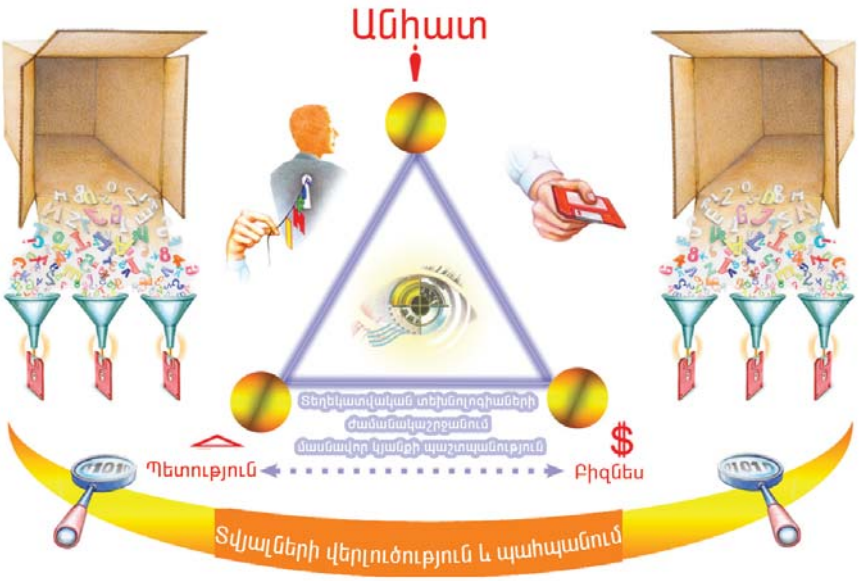
իրավունքն է: Այն ճանաչված է Մարդու իրավունքների համընդհանուր հռչակագրում, Քաղաքացիական և քաղաքական իրավունքների մասին միջազգային պայմանագրում ու մարդու իրավունքների հարցերի վերաբերյալ բազում այլ միջազգային և տարածաշրջանային պայմանագրերում: «Մասնավոր կյանք» հասկացության սահմանները կախված են ազգային մշակույթի և կենսակերպի տարբերություններից: Գաղտնիության, մասնավորության պահպանման հիմնախնդիրը, որն շատ կարևոր է արևմտյան հասարակության համար, կարող է այնքան էլ կարևոր չլինել այլ երկրների մշակույթներում: Այդ հասկացության արդի սահմանումը շեշտադրում է հեռահաղորդակցությունների գաղտնիության (գրագրությանը չհետևել) և մասնավոր տեղեկատվության պահպանման վրա (մասնավոր անձանց մասին չբացահայտված տեղեկատվություն): Մասնավոր կյանքի գաղտնիքի պահպանումը, որն ավանդաբար վերաբերում էր հիմնականում պետության գործողություններին, այսօր ավելի ընդարձակվել է և, ինչպես ստորև ներկայացված է նկարում, ընդգրկում է գործնական սեկտոր[22]:

Մասնավոր կյանքի գաղտնիքը. մասնավոր անձինք եւ պետություններ

Իշխանական մարմինների համար տեղեկատվությունը միշտ եղել է տարածքներն ու բնակչությանը վերահսկելու կարևորագույն գործիքը: Կառավարությունները հավաքում են անձնական մեծածավալ տեղեկություններ (ծնունդների եւ ամուսնությունների գրանցման, անձնագրերի համարների, քվեարկությունների, դատվածության մասին տվյալներ, հարկային տեղեկատվություն, բնակարանային հաշվառման տվյալներ, մեքենաների գրանցման մասին տվյալներ և այլն): Քաղաքացիները հնարավորություն չունեն այդպիսի տեղեկատվություն տրամադրելուց հրաժարվելու, եթե, իհարկե, չեն տարագրվում այլ երկիր, որտեղ նրանք, միևնույն է, բախվելու են այդ հիմնախնդիրներին: Տվյալների խորքային մշակման համար կիրառվող տեղեկատվական տեխնոլոգիաները հնարավորություն են տալիս ամբողջացնելու տարբեր համակարգերի տվյալները (օրինակ՝ հարկային, բնակարանների և մեքենաների հաշվառման)՝ բարդ վերլուծական ընթացակարգեր անցկացնելու, կրկնվող մոդելների որոնման և անհամապատասխանությունների բացահայտման համար:

Էլեկտրոնային կառավարման բնագավառում ցանկացած նախաձեռնության համար հիմնական բարդություններից մեկը կառավարական գործառույթների արդիականացման և քաղաքացիների մասնավոր կյանք ունենալու իրավունքների երաշխիքներն ապահովելու միջև պատշաճ հավասարակշռության ապահովումն է:

2011 թ. սեպտեմբերի 11-ից հետո ԱՄՆ-ում ընդունված «Հայրենասիրական գործողություն» (Patriot Act) և նմանատիպ օրենքներն այլ երկրներում ընդլայնեցին կառավարության մարմինների լիազորությունները



տեղեկատվություն հավաքելու ոլորտում, ներառյալ տեղեկատվությունը օրինականորեն խափանելու իրավունքը[23]: Հանցանշաններ հավաքելու նպատակով օրինականորեն խափանելու հայեցակարգը ընդգրկված է նաև կիբեռհանցագործության մասին Եվրախորհրդի պայմանագրում (էջ՝ 20 և 21):

Մասնավոր կյանքի գաղտնիության պահպանումը. մասնավոր անձինք և բիզնեսը

Մասնավոր կյանքի գաղտնիության պահպանման տարբեր բաղադրիչները պատկերող Եռանկյունու երկրորդ կողմը (տես նկարը) մասնավոր անձանց և բիզնես-հատվածի փոխհարաբերություններն են: Յուրաքանչյուր մարդ իր մասին անձնական տվյալներ է հայտնում բանկում հաշիվ բացելով, ամրագրելով ավիատոմս կամ հյուրանոցի համար, համացանցում վարկային քարտով վճարումներ կատարելով և պարզապես համացանցում աշխատելով: Այս իրավիճակներից ամեն մեկում բազմաթիվ «հետքեր» են մնում: Տեղեկատվական տնտեսության մեջ հաճախորդների մասին տվյալները, այդ թվում նրանց նախընտրություններն ու գնումներ կատարելու յուրահատկությունները կարևոր ապրանք են դառնում: Որոշ ընկերությունների համար, ինչպիսիք են՝ Google-ը և Amazon-ը հաճախորդների նախասիրությունների մասին տեղեկատվությունը բիզնես-մոդելի անկյունաքարն է համարվում: Էլեկտրոնային առևտրի հաջողությունն ու կայունությունը ինչպես կազմակերպությունների միջև, այնպես էլ կազմակերպությունների ու մասնավոր անձանց միջև կախված է մասնավոր կյանքի գաղտնիության ապահովման քաղաքականության և անվտանգության միջոցառումների հանդեպ վստահությունից, որոնք ձեռնարկվում են հաճախորդների մասին գաղտնի տեղեկատվությունը կողոպուտից ու չարաշահումներից պաշտպանելու համար24: Սոցիալական

ցանցերի տարածման հետ միասին ի հայտ է գալիս երկյուղ այն մասին, որ կգա մի ժամանակ, երբ դրանցում պահվող անձնական տվյալներն ոչ միայն այդ ծառայությունների սեփականատերերը կամ նրանց ադմինիստրատորներն, այլև այդ ցանցերի այլ օգտատերեր կարող են օգտագործել այլ նպատակներով:

Մասնավոր կյանքի գաղտնիքի պահպանումը. պետությունն ու բիզնեսը

Եռանկյունու երրորդ կողմի մասին քիչ բան է հայտնի (տես նկ. 145), թեև այն, միգուցե, մասնավոր կյանքի գաղտնիքի պահպանմանը վերաբերող ամենակարևոր տեսանկյունն է: Երկու կողմերն էլ՝ և պետությունը, և բիզնեսը, մասնավոր անձանց մասին մեծածավալ տեղեկատվություն են հավաքում: Տվյալների մի մասը նրանք փոխանցում են այլ պետությունների և ընկերությունների՝ ահաբեկչական գործողությունները կանխելու նպատակով: Սակայն որոշ իրավիճակներում, օրինակ՝ տվյալների գաղտնիության պահպանման վերաբերյալ Եվրոպական հրամանագրում նախատեսված իրավիճակների դեպքում, պետությունը պահպանում է առևտրային կառույցների ենթակայության ներքո գտնվող քաղաքացիների մասին տեղեկատվությունը:

Մասնավոր կյանքի գաղտնիության պահպանումը. քաղաքացիներ

Մասնավոր կյանքի գաղտնիքի պահպանման վերջին տեսակետը, որը չի ընդգրկվել 145-րդ էջի եռանկյունու մեջ, առանձին քաղաքացիներից բխող գաղտնիության հավանական վտանգն է: Այսօր ամեն մարդ, ով բավականաչափ հնարավորություններ ունի, կարող է ձեռք բերել լրտեսման հզոր գործիքներ: Նույնիսկ տեսախցիկներով հասարակ բջջային հեռախոսները կարող են դառնալ լրտեսման միջոցներ: «The Economist» ամսագրի հեղինակներից մեկի արտահայտմամբ, տեխնոլոգիան «ազատականացրել է լրտեսումը»: Մարդկանց մասնավոր կյանքի անձեռնմխելիության խախտման շատ դեպքեր են հայտնի. այդպիսիք են հարևաններին հետևելու պարզ ձևերից մինչև բանկային քարտերի համարների գրանցման և էլեկտրոնային լրտեսության նպատակով տեսախցիկների ավելի հնարամիտ օգտագործումը: Այդպիսի խախտումներից պաշտպանվելու տեսակետից հիմնական բարդությունն այն է, որ օրենսդրական կարգերի մեծ մասը վերաբերում է պետության գործողություններից մասնավոր կյանքի գաղտնիքը պահելուն: Վերը նշված նոր երևույթներին բախվելով, որոշ երկրներ սկսեցին ձեռնարկել համապատասխան քայլեր: ԱՄՆ Կոնգրեսը այլատարությունը կանխող փաստաթուղթ է ընդունել, որն արգելում է մարդկանց մերկ նկարել, առանց նրանց համաձայնության: Գերմանիան և մի շարք այլ երկրներ նույնպես նմանատիպ օրենքներ են ընդունել, որոնք արգելում են մասնավոր անձանց լրտեսման հնարավորություններն օգտագործել այլ մարդկանց նկատմամբ:

Մասնավոր կյանքի գաղտնիության պահպանման և գաղտնի տվյալների միջազգային կարգավորումը

Մասնավոր կյանքի գաղտնիության և գաղտնի տվյալների պահպանումը կարգավորող միջազգային հիմնական փաստաթղթերից է 1981 թ. Եվրախորհրդի ընդունած անձնական տվյալների ավտոմատ մշակման ընթացքում ֆիզիկական անձանց պաշտպանության մասին պայմանագիրը25: Պայմանագիրը բաց է մյուս պետությունների, այդ թվում նաև Եվրախորհրդին չանդամակցած պետությունների ստորագրման համար: Քանի որ այդ պայմանագիրը տեխնիկապես չեզոք է, այն ենթարկվել է ժամանակի փորձությանը: Վերջին ժամանակներում այն դիտարկում են որպես կենսաչափական տվյալների հավաքագրումն ու մշակումը կիրառելու գործիք: Եվրամիությունում անձնական տվյալների մշակման համար իրավական հիմքը սահմանված է Տվյալների պահպանման մասին ԵՄ հրահանգում (Directive 45/46/ԵՄ), որը մեծ ազդեցություն է գործել ԵՄ և դրա սահմաններից դուրս ազգային օրենսդրությունների վրա: Մասնավոր կյանքի գաղտնիքի և անձնական տվյալների պահպանման հարցերին վերաբերող մեկ այլ կարևոր, սակայն պարտադրող բնույթ չունեցող միջազգային փաստաթուղթ է 1980 թ. Տնտեսական համագործակցության և զարգացման կազմակերպության (ՏՀԶԿ) ստեղծած «Մասնավոր կյանքի գաղտնիքի և անձնական տվյալների արտասահմանյան հոսքերի գաղտնիության պահպանման հիմնական սկզբունքները»: Այդ սկզբունքները և դրանց հաջորդած ՏՀԶԿ-ի մյուս աշխատանքը նպաստեցին, որ այդ ոլորտում միջազգային և տարածաշրջանային շատ կարգեր ստեղծվեն: Ներկայում ՏՀԶԿ համարյա բոլոր երկրները մասնավոր կյանքի պահպանման ոլորտում օրենսդրություն են ստեղծել և իշխանական մարմիններին տվել են համապատասխան լիազորություններ: ՏՀԶԿ առաջարկած սկզբունքները, թեև ընդունվել են շատ երկրներում և տարածաշրջաններում, սակայն դրանց կիրառման միջոցները տարբեր են: Օրինակ՝ եվրոպական և ամերիկյան մոտեցումներն այդ հարցում զգալիորեն տարբերվում են: Եվրոպայում տվյալների պահպանման օրենսդրությունը համապարփակ է, իսկ ԱՄՆ-ում գաղտնիությանը վերաբերող իրավակարգերը գործունեության յուրաքանչյուր ոլորտի համար առանձին են մշակվում: Ֆինանսական գաղտնիքի ոլորտում այն «Գրեմ Լիչ-Բլայլի 26 փաստաթուղթ»-ն է, երեխաների վերաբերյալ գաղտնիության ոլորտում՝ «Առցանց երեխաների մասնավոր կյանքի պաշտպանության մասին» փաստաթուղթը27, բժշկական տեղեկատվության գաղտնիությունն ապահովելու է առողջապահության ու սոցիալական ապահովության մասին վերջերս առաջարկված օրենքների փաթեթը28:

Մեկ այլ կարևոր տարբերություն է այն, որ Եվրոպայում օրենքների պահպանմանը հետևում են պետական մարմինները, իսկ ԱՄՆ-ում դրանց կատարումն ապահովվում է մասնավոր սեկտորի միջոցով և ինքնակարգավորման հիման վրա: Գաղտնիությունն ապահովելու քաղաքականությունը սահմանում են ընկերությունները, իսկ մասնավոր անձինք ինքնուրույն են որոշում՝ ընդունել դրանք թե ոչ: ԱՄՆ-ի այս

մոտեցման դեմ գլխավոր փաստարկն այն է, որ սպառողները գտնվում են անբարենպաստ դրության մեջ: Մասնավոր անձինք, որպես կանոն, հաշվի չեն առնում, թե որքան կարևոր են գաղտնիության քաղաքականության թվարկված պայմանները, և դրանք ընդունում են առանց կարդալու:

ԵՄ և ԱՄՆ միջև «Հուսալի հանգրվանի» մասին համաձայնագիրը

Այս երկու՝ եվրոպական և ամերիկյան մոտեցումների միջև հակասություններ են ծագել: Այդ խնդրի հիմնական աղբյուրը դարձավ անձնական տվյալները առևտրային կառույցների կողմից օգտագործումը:

ԵՄ-ն ինչպե՞ս կարող է ապահովել իր սահմանած կարգերի պահպանումը, ենթադրենք՝ ԱՄՆ-ում տեղակայված ծրագրային ապահովում արտադրող ընկերության կողմից: Ինչպե՞ս կարող է ԵՄ-ն երաշխավորել, որ ԵՄ քաղաքացիների մասին տեղեկատվությունը պահպանվում է «Տվյալների պահպանման մասին» հրահանգում շարադրված սկզբունքներին համապատասխան: Ի՞նչ կարգադրությունների համաձայն (ամերիկյան կամ եվրոպական) պետք է դիմել ԵՄ-ից ԱՄՆ կորպորատիվ ցանցերով ընկերություն փոխանցվող տեղեկատվության վերաբերյալ: Եվրամիությունը սպառնում էր ուղեփակել տվյալների փոխանցումը այն երկրներ, որտեղ ընդունակ չեն հրահանգի համաձայն ապահովելու տեղեկատվության պահպանման մակարդակը: Այս դիրքորոշումը հանգեցրեց անխուսափելի բախման ամերիկյան մոտեցման հետ: Մոտեցումների խորքային տարբերությունները խոչընդոտում էին որևէ համաձայնության հասնելուն: Ավելին, ամերիկյան օրենքները եվրոպականին հարմարեցնելն անհնար էր, քանի որ դա կպահանջեր ամերիկյան իրավական համակարգի արմատական որոշ սկզբունքների փոփոխություն: Այդ իրավիճակից ելքը գտնվեց այն ժամանակ, երբ ԱՄՆ դեսպան Դևիդ Ահարոնը առաջարկեց «հուսալի հանգրվանի» բանաձևը: Այդ առաջարկը հիմնախնդիրը ներկայացնում էր նոր լույսի ներքո և հնարավորություն տվեց դիվանագիտական փակուղուց դուրս գալու: Գտնվեց մի որոշում, որի առկայությամբ ԵՄ կարգերը իրավական «հանգրվանում» կարող են կիրառվել ԱՄՆ ընկերությունների նկատմամբ: Եվրամիության երկրների քաղաքացիների մասին տվյալների հետ աշխատող ամերիկյան ընկերությունները կարող են կամովի կատարել ԵՄ-ում ընդունված գաղտնիության պահպանման մասին պահանջները: Համապատասխան համաձայնագրերը ստորագրելով, ընկերությունները պետք է հետևեն դրանց կատարման պաշտոնապես ընդունված մեխանիզմներին, որոնք համաձայնեցված են ԱՄՆ և ԵՄ միջև:

2000 թ. երբ ստորագրվեց «հուսալի հանգրվանի» մասին համաձայնագիրը, մեծ հույսեր կապվեցին դրա հետ՝ որպես մի գործիքի, որը կարող է օգնել լուծելու նմանատիպ հիմնախնդիրները այլ երկրների նկատմամբ: Սակայն դեռևս համաձայնագրի արդյունավետությունն այնքան էլ տպավորիչ չէ: Եվրախորհրդարանը այն քննադատել է՝ ԵՄ քաղաքացիների մասին տվյալների գաղտնիության պատշաճ մակարդակ չապահովելու համար: Ամերիկյան ընկերությունները նույնպես շահագրգռված չեն այդ մոտեցման հարցում: Galexia

ընկերության վերջերս կատարած հետազոտության համաձայն, «հուսալի հանգրվանի» մասին համաձայնագիրն ընդունած 1597 ընկերությունից միայն 348-ն է համապատասխանում նրա հիմնական պահանջներին (օրինակ՝ գաղտնիության քաղաքականությանը) 29: Հաշվի առնելով Եվրամիության համար գաղտնիության և տվյալների պահպանման հարցերի կարևորությունը, եվրոպական քաղաքագետները, հավանաբար, պետք է մի նոր բանով փոխարինեն այլևս չաշխատող «հուսալի հանգրվանի» մասին համաձայնագիրը:

Բազմալեզվություն և մշակութային բազմազանություն

Իր գոյության առաջին օրերից համացանցը առավելապես անգլալեզու միջավայր էր: Վիճակագրության համաձայն, համացանցի բովանդակության մոտավորապես 80 տոկոսը անգլերենով նյութերն են, թեև Երկրագնդի բնակչության 80 տոկոսն այլ լեզուներով է խոսում: Այդ իրավիճակը սթափեցրեց շատ երկրների, որպեսզի համաձայնեցված միջոցներ ընդունեն՝ բազմալեզվությունը պահպանելու և մշակութային բազմազանությունը պաշտպանելու նպատակով: Բազմալեզվությանն աջակցելու խնդիրը ոչ միայն մշակութային առանձնահատկությունների պահպանումն էր, այլև կապված էր հմացանցի հետագա զարգացման հեռանկարների հետ30: Որպեսզի համացանցից օգտվել կարողանան ոչ միայն էլիտան, այլև բնակչության ավելի լայն շերտերը, նյութերը պետք է մատչելի ու հասանելի լինեն տարբեր լեզուներով:

Հարցեր

Առաջին՝ բազմալեզվության զարգացումը պահանջում է տեխնիկական ստանդարտների առկայություն, որը հնարավորություն կտա բացի լատինատառից օգտագործել նաև այլ այբուբեններ: Այդ ոլորտում առաջին նախաձեռնություններից մեկը Unicode կոնսորցիումինն էր՝ ոչ առևտրային կազմակերպություն, որը մշակում է ստանդարտներ՝ տարբեր այբուբենների խորհրդանիշերը կիրառելու համար: ICANN և IETF կազմակերպություններն, իրենց հերթին, չինարենով, արաբերենով և այլ լեզուներով միջազգային դոմենային անվանումների առաջխաղացմանն ուղղված կարևոր միջոցներ ձեռնարկեցին:
Երկրորդ՝ բազմաթիվ փորձեր են արվել բարելավելու մեքենայական թարգմանությունները: Եվրամիության կանոնների համաձայն, պաշտոնական փաստաթղթերը պետք է թարգմանվեն բոլոր անդամ պետությունների լեզուներով, այդ առնչությամբ ԵՄ-ն աջակցում էր մեքենայական թարգմանությունների կատարելագործմանն ուղղված տարբեր նախագծերին: Չնայած կասկած չհարուցող հաջողություններին, այդ ոլորտում հաջողությունները հիմնականում բավականին սահմանափակ են:

Երրորդ՝ բազմալեզվության զարգացումը պահանջում է համապատասխան կանոնավորող շրջանակների ստեղծում: Այդ ոլորտում կարևոր դեր է կատարում ՅՈւՆԵՍԿՕՆ, որը բազմալեզվության զարգացման վերաբերյալ մի քանի նախագծեր է նախաձեռնել և ընդունել է մի շարք արմատական փաստաթղթեր, մասնավորապես, Մշակութային բազմազանության մասին համընդհանուր հռչակագիրը: Այդ ոլորտում ակտիվ աշխատող մեկ այլ կազմակերպություն է Եվրամիությունը, որը բազմալեզվությունը հռչակում է որպես իր քաղաքական և աշխատանքային գլխավոր սկզբունքներից մեկը: Վեբ 2.0 գործիքների զարգացումն ու լայնորեն կիրառումը, որոնք սովորական օգտատերերին հնարավորություն են ընձեռում համացանցում նյութերի տեղադրման գործում իրենց ավանդն ունենալու, տարբեր լեզուներով տեղական բովանդակությամբ նյութերի քանակի և ծավալի ավելացման հեռանկարներ է բացում: Սակայն առանց բազմալեզվության առաջխաղացման համընդհանուր քաղաքականության և դրական «հետադարձ կապի» բացակայության պայմաններում այդ հնարավորությունները կարող են հանգեցնել լեզվական ճեղվածքի մեծացման: «Համացանցի նոր օգտատերերը տեսնում են, թե ինչ օգտակար է անգլերենի իմացությունը և այն առցանց հեռահաղորդակցությունների համար կիրառելը, ինչն էլ բարձրացնում է լեզվի վարկը և ստիպում է, որ օգտատերերի ապագա սերունդները սովորեն այդ լեզուն»[31]:

Համաշխարհային հասարակական բարիքներ

Համաշխարհային հասարակական բարիքների հայեցակարգը կապված է համացանցի կառավարման շատ տեսակետների հետ: Այն անմիջական կապ ունի այնպիսի տեսակետների հետ, ինչպիսիք են՝ համացանցի ենթակառուցվածքին հասանելիությունը, համացանցում փոխհարաբերությունների արդյունքում ստեղծված գիտելիքների պահպանությունը, բաց տեխնիկական ստանդարտների պահպանությունը և առցանց կրթությանը հասանելիության իրավունքը: Համացանցի ենթակառուցվածքը վերահսկում են առավելապես մասնավոր ընկերությունները: Ընթացիկ խնդիրներից մեկը համացանցի ենթակառուցվածքի և դրա համաշխարհային հասարակական բարիքի կարգավիճակի հետ մասնավոր սեփականության ներդաշնակության որոնումն է: Պետական օրենքները հնարավորություն են տալիս սահմանափակելու մասնավոր սեփականության իրավունքը՝ հասարակական շահերից բխող որոշակի պահանջների օգնությամբ, ինչպիսիք են՝ հավանական բոլոր օգտատերերին հավասար իրավունքների տրամադրումը և փոխանցվող նյութերի բովանդակությանը չմիջամտելը: Համացանցի կարևորագույն առանձնահատկություններից է ողջ աշխարհի օգտատերերի փոխհարաբերությունների արդյունքում նոր գիտելիքների և տեղեկատվության ստեղծումը: Գիտելիքների զգալի ծավալը ստեղծվել է էլեկտրոնային

հաղորդագրությունների փոխանակման ընթացքում, սոցիալական ցանցերի և բլոգների միջոցով: Բացառությամբ Creative Commons արտոնագրի, այդ գիտելիքները պահպանելու իրավական մեխանիզմներ գոյություն չունեն: Առանց պատշաճ իրավական կարգավորման այդ գիտելիքները կարող են վերածվել ապրանքի, վաճառքի առարկայի: Այդպիսով, ստեղծագործական գործունեության համար կարևոր հիմք համարվող գիտելիքների ընդհանուր պաշարը կարող է սպառվել: Համացանցի նյութերը որքան շահույթի աղբյուր են դառնում, ըստ այդմ ավել ու ավելի է բարդանում տեղեկատվության ազատ փոխանակում իրականացնելը, ինչը կարող է հանգեցնել ստեղծագործական փոխգործողությունների կրճատման: Համաշխարհային հասարակական բարիքի հայեցակարգը այնպիսի նախաձեռնությունների հետ միասին, ինչպիսին է Creative Commons-ը, կարող է տալ այնպիսի լուծումներ, որոնք ունակ են պահպանելու համացանցի ստեղծագործական ներուժը և պահելու դրանում ստեղծված գիտելիքները՝ ապագա սերունդների համար: Ստանդարտների ոլորտում նույնպես բազմաթիվ փորձեր են ձեռնարկվում հասարակական, բաց ստանդարտները մասնավորի և սեփականատիրականի փոխարինելու: Այդպես եղավ Microsoft (ASP և զննարկիչների նկատմամբ կիրառված) և Sun Microsystems (օրինակ՝ Java) ընկերությունների հետ: Համացանցի ստանդարտները (հիմնականում՝ TCP/IP) համարվում են բաց և հասարակական: Համացանցի կառավարման կարգը պետք է ապահովի համացանցի հիմնական ստանդարտների՝ որպես համաշխարհային հասարակական բարիքի պահպանությունը:

Հարցեր

Մասնավոր և հասարակական շահերի միջև հավասարակշռությունը

Համացանցի հետագա զարգացման հետ կապված հիմնական խնդիրներից մեկը մասնավորի և հասարակական շահերի միջև հավասարակշռության որոնումն է: Հարցն այն է, թե ինչպես մասնավոր սեկտորի համար բարենպաստ պայմաններ ստեղծել, միաժամանակ ապահովելով համացանցի զարգացումը՝ որպես համաշխարհային հասարակական բարիք: Շատ դեպքերում դա «զրոյական ելքով խաղ չէ», այլ մի իրավիճակ, երբ բոլորը կարող են շահել: Google-ը և Վեբ 2.0-ի շատ ուրիշ ընկերություններ կարողացել են մշակել այնպիսի բիզնես մոդելներ, որոնք միաժամանակ շահույթ են բերում և համացանցի ստեղծագործական զարգացման համար հնարավորություններ են տրամադրում:

Համացանցի՝ որպես համաշխարհային հասարակական բարիքի պահպանումը[32]

Որոշ լուծումներ կարող են մշակվել գոյություն ունեցող տնտեսական և իրավական հայեցակարգերի հիման վրա: Օրինակ՝ տնտեսագիտության տեսության մեջ գոյություն ունի հասարակական բարիքների լավ զարգացած հայեցակարգ, որը միջազգային մակարդակում ընդարձակվել է և հասել

մինչև համաշխարհային հասարակական բարիքի: Հասարակական բարիքն ունի երկու կարևոր բնութագիր՝ անմրցունակ սպառում և ոչ բացառիկություն: Առաջինը ենթադրում է, որ բարիքի սպառումը մեկ անձի կողմից չի նսեմացնում այդ բարիքը մյուսների սպառման համեմատ: Երկրորդը նշանակում է, որ դժվար է, նույնիսկ անհնար է որևէ մեկին խանգարել բարիքից օգտվել: Համացանցի նյութերին և համացանցային շատ այլ ծառայություններին հասանելիության իրավունքը համապատասխանում է նշված երկու չափանիշներին՝ սպառման մեջ անմրցունակություն և տրամադրման հարցում ոչ բացառիկություն:

Սահմանափակ ֆիզիկական հնարավորություններով մարդկանց իրավունքները[33]

ՄԱԿ-ի գնահատականների համաձայն, աշխարհում սահմանափակ հնարավորություններով 500 մլն մարդ է ապրում: Այս թիվն անընդհատ ավելանում է պատերազմների, կյանքի անբարենաստ պայմանների, հիվանդությունների, դրանց պատճառների, կանխման և բուժման մասին գիտելիքների պակասի պատճառով[34]: Համացանցը հաշմանդամներին հասարակության կյանքում ներգրավվելու նոր հնարավորություններ է տալիս: Սահմանափակ հնարավորություններով մարդկանց օգնելու տեսանկյունից տեխնոլոգիաների ներուժը առավելագույնի հասցնելու համար, անհրաժեշտ է մշակել համացանցի կառավարման համապատասխան մոդել: Այդ բնագավառում միջազգային հիմնական գործիքը 2006 թ. ՄԱԿ-ի ընդունած Հաշմանդամների իրավունքների մասին պայմանագիրն է, որն արդեն 139 երկիր ստորագրել է: Այդ պայմանագրում ամրագրված իրավունքները ներկայում ընդգրկվում են ազգային օրենսդրությունների համակարգերում, ինչը մի քանի տարի հետո հնարավորություն կտա ապահովել դրանց կիրառումը[35]:
Սահմանափակ հնարավորություններով մարդկանց պահանջները հաշվի առնելու անհրաժեշտության գիտակցումը տեխնոլոգիական լուծումները նախագծելիս աստիճանաբար աճում է շնորհիվ այնպիսի կազմակերպությունների, ինչպիսիք են Սահմանափակ հնարավորությունների և հասանելիության իրավունքի հարցերով IGF դինամիկ կոալիցիան և Համացանցի հասարակության սահմանափակ հնարավորությունների ու հատուկ պահանջարկների գծով բաժանմունքը[37]: Հաշմանդամները հաճախ զրկված են լինում սարքերի, համացանցի ծրագրային ապահովման և նյութերի օգտագործման համար անհրաժեշտ ունակություններից: Համապատասխան հնարավորություններ կարելի է ստեղծել երկու ուղղությամբ տարվող աշխատանքների շնորհիվ: Առաջին՝ սարքավորումների դիզայնի, ԾԱ և նյութերի հանդեպ պահանջների մեջ անհրաժեշտ է ներառել հասանելիության ստանդարտները: Երկրորդ՝ պետք է բարձրացնել օգտատերերի որոշակի ֆիզիկական ունակություններն ուժեղացնող կամ փոխարինող լրացուցիչ սարքավորումների և ԾԱ հասանելիությունը: Համացանցի կառավարման տեսանկյունից ուշադրության կենտրոնում են գտնվում կոնտենտը և

ծառայությունները, քանի որ դրանց ծավալն ու քանակը արագ մեծանում են և միասին ստեղծում են յուրատեսակ ենթակառուցվածք: Շատ վեբ-հավելվածներ չեն համապատասխանում հասանելիության ստանդարտներին դրանք մշակողների վատ իրազեկվածության և անհրաժեշտ լուծումների ենթադրյալ բարդության ու բարձր արժեքի մասին ներկա իրողություններին չհամապատասխանող պատկերացումների պատճառով:
Համացանցի համար հասանելիության միջազգային ստանդարտները մշակել է «համաշխարհային սարդոստայնի» (W3C) կոնսորցիումը և կոչվում են «Վեբ-կոնտենտի հասանելիության ուղեցույց»[38]: Սահմանափակ հնարավորություններով մարդկանց հասանելիության իրավունքը գլոբալ ցանցի ծառայությունների ու նյութերի նկատմամբ ընդարձակելուն կոչված նախաձեռնություններից մեկը «Համացանցի համապարփակ դիզայն» աշխատությունն է, որն առաջարկել է Համացանցի միությունը (Internet Society) և ձևակերպվում է հետևյալ կերպ. «Համացանցի համապարփակ դիզայնը նյութերի տրամադրման և տեխնոլոգիական դիզայնի առումով նշանակում է ճկունության ապահովում, որպեսզի հաշվի առնվի օգտատերերի առավելագույն մեծ լսարանի պահանջները, անկախ տարիքից, լեզվից, ֆիզիկական ունակություններից»[39]:

Կրթություն

Համացանցը նոր հնարավորություններ է ստեղծել կրթության համար: Անընդհատ ի հայտ են գալիս նոր նախաձեռնություններ էլեկտրոնային կրթության, առցանց կրթության, հեռավորության վրա վարվող կրթության բնագավառներում, որոնց հիմնական նպատակը համացանցը որպես ուսուցման միջոց օգտագործելն է:

Առցանց կրթությունը, թեև չի կարող փոխարինել ավանդական ուսուցմանը, սակայն այն նոր հնարավորություններ է տալիս այնպիսի դեպքերում, երբ ժամանակը կամ տարածությունը դժվարացնում են պարապմունքներին հաճախել (առկա ուսուցում): Որոշ ուսումնասիրություններ ցույց են տվել, որ առցանց կրթության շուկան շարունակելու է ավելի աճել, մոտավորապես հասնելով ԱՄՆ 10 մլրդ դոլարի: Կրթության բնագավառում ավանդական կարգավորող շրջանակները սահմանել են պետական կառույցները: Կրթական հիմնարկների հավաստագրումը, աստիճանների շնորհումը և կրթության որակի ապահովումը կարգավորվում են պետական մակարդակով: Սակայն միջազգային կրթությունը պահանջում է կառավարման նոր կարգերի ստեղծում: Միջազգային շատ նախաձեռնություններ ձգտում են լրացնել կառավարման ոլորտում գոյություն ունեցող դատարկությունը, հատկապես դիպլոմների և աստիճանների շնորհման և որակավորման վերահսկողության մասով:

Հարցեր

ԱՀԿ-ն և կրթությունը

ԱՀԿ շրջանակներում բանակցությունների հակասական տեսակետներից է Ծառայությունների առևտրի վերաբերյալ գլխավոր պայմանագրի (GATS) 1(3) (b) և (c) հոդվածների մեկնաբանությունը, որը պետության տրամադրած ծառայությունների համար ազատ առևտրի ռեժիմից բացառություններ է նախատեսում: Տեսակետներից մեկի համաձայն, որը պաշտպանում են հիմնականում ԱՄՆ-ն և Մեծ Բրիտանիան, այդ բացառությունները պետք է մեկնաբանվեն նեղ իմաստով, և բարձրագույն կրթության ոլորտում դե ֆակտո պետք է իրականացվի ազատ առևտուր: Այս մոտեցումը գլխավորապես թելադրված է կրթական ծառայությունների համաշխարհային շուկայի ձևավորման հարցում ԱՄՆ և Մեծ Բրիտանիայի կրթական սեկտորի շահերով, և առաջ է բերում այլ պետությունների բազմաթիվ առարկությունները:

ԱՀԿ և միջազգային այլ կազմակերպությունների շրջանակներում հետագա քննարկումներն անցկացվելու են կրթության բնույթի մասին. այն արդյոք ապրանք է, թե հասարակական բարիք: Կրթությունը եթե դիտարկենք որպես ապրանք, ապա ազատ առևտրի կանոնները, որ ընդունել է ԱՀԿ-ը, կարելի կլինի նաև այդ բնագավառում կիրառել: Իսկ եթե կրթությանը վերաբերվենք որպես հասարակական բարիքի, ապա կպահպանվի կրթության գոյություն ունեցող մոդելը, որի համաձայն պետական համալսարաններն ունեն ազգային մշակույթի համար կարևոր հատուկ հիմնարկությունների կարգավիճակ:

Որակի ապահովումը

Էլեկտրոնային կրթության բնագավառում ծառայություններ տրամադրելու համար անհրաժեշտ գործիքների մատչելիությունը և հեշտորեն այդ շուկա մուտք գործելու հանգամանքը որակի վերահսկողության հետ կապված մի շարք հարցեր են առաջադրում: Առցանց ավելի ու ավելի շատ նյութեր ներկայացնելու ձգտումը կարող է հանգեցնել ուսումնական նյութերի և ուսուցողական մեթոդների որակազրկման: Բացի այդ, կրթության որակի վրա մի շարք գործոններ կարող են բացասաբար ազդել: Դրանցից մեկը շուկայում նոր, հիմնականում առևտրային ուղղվածության կրթական հիմնարկությունների ի հայտ գալն է, որոնցից շատերը չեն տիրապետում անհրաժեշտ ակադեմիական և ուսուցողական կարողությունների: Որակի ապահովման մեկ այլ հիմնախնդիր է այն, որ նյութերը թղթից առցանց միջավայր փոխադրելիս ուսուցողական ներուժը չի օգտագործվում: Բացի այդ, կրթության որակի վրա մի շարք գործոններ կարող են բացասաբար ազդել: Դրանցից մեկը շուկայում նոր, հիմնականում առևտրային ուղղվածության կրթական հիմնարկությունների ի հայտ գալն է, որոնցից շատերը չեն տիրապետում անհրաժեշտ ակադեմիական և ուսուցողական կարողությունների: Որակի ապահովման մեկ այլ հիմնախնդիրն այն է,

որ նյութերը թղթից առցանց միջավայր փոխադրելիս դրա ուսուցողական ներուժը չի օգտագործվում:

Ակադեմիական կոչումների շնորհումն ու ստուգարքային միավորների ընդհանուր համակարգի ստեղծումը

Առցանց ուսուցման ոլորտի առնչությամբ առանձնակի կարևորություն ունի գիտական աստիճանների շնորհման հարցը: Այս հարցում հիմնական խնդիրը կոնկրետ տարածաշրջանի սահմաններից դուրս, առաջին հերթին, համաշխարհային մակարդակով դիպլոմների եւ գիտական աստիճանների ճանաչումն ապահովելն է: ԵՄ-ն սկսել է այդպիսի կանոնակարգող բազայի մշակումը՝ որպես վարկերի փոխստուգարքային համակարգ: Ասիա-խաղաղօվկիանոսյան տարածաշրջանը հետևում է Եվրոպայի օրինակին՝ ստեղծելով ուսանողների փոխանակման համար և ստուգարքային միավորների համակարգի (UCTS) իր սեփական տարածաշրջանային մոդելը:

Առցանց ուսուցման ստանդարտացումը

Առցանց ուսուցման զարգացման նախնական փուլը տեխնիկական լուծումների, բովանդակության և ուսուցման առումով բնութագրվում էր արագ զարգացմամբ և նյութերի բազմազանությամբ: Սակայն առցանց դասընթացների փոխանակումը հեշտացնելու և որակի որոշակի ստանդարտի արմատավորման նպատակով անհրաժեշտ է մշակել ընդհանուր ստանդարտներ: Ստանդարտացման ամենամեծ ծավալի աշխատանքները կատարում են ԱՄՆ մասնավոր և արհեստավարժ հիմնարկությունները: Մյուս նախաձեռնությունները, ներառյալ միջազգայինը, փոքրածավալ են:

Համացանցում երեխաների անվտանգությունը[40]

Երեխաները հաճախ են զոհի դերում հայտնվում: Համացանցում անվտանգությանն առնչվող հարցերի մեծ մասը վերաբերում է երիտասարդներին, հատկապես անչափահասներին: Թույլատրելիի և անթույլատրելիի միջև սահմանը ավելի ակնհայտ է դառնում, երբ խոսքը երեխաների անվտանգությանն է վերաբերում:

«Կիբեռահաբեկում» - Ոտնձգությունն ավելի կարևոր հիմնախնդիր է դառնում, երբ թիրախ են դառնում անչափահասները: Հեռահաղորդակցային կապի տարբեր միջոցներից, ինչպիսիք են՝ հաղորդագրությունների փոխանակման համակարգը, չաթերը և սոցիալական ցանցերը, ամենաակտիվ օգտվողները երեխաներն ու երիտասարդությունն է, որոնք էլ ամենախոցելիներն են: Երեխաները շատ հեշտ համացանցում դառնում են ահաբեկումների զոհեր, հատկապես այն հասակակիցների կողմից, ովքեր որպես գործիք օգտագործում են տեղեկատվա-հեռահաղորդակցային տարբեր տեխնոլոգիաներ:

Բռնություն և սեռական շահագործում

Անչափահասներին ուղղված այս գործողությունները հատկապես վտանգավոր են, երբ դրանք իրականացնում են մեծերը: Ավելի հաճախ համացանցային մանկապիղծները թաքցնում են իրենց անձը և հանդես գալով որպես հասակակից, տեղեկություններ են հավաքում ու աստիճանաբար փորձում են գրավել երեխայի վստահությունը, նույնիսկ պայմանավորվել հանդիպման մասին: Այդպիսով, վիրտուալ գործողությունները վերածվում են իրական շփման և կարող են հանգեցնել այնպիսի հետևանքների, ինչպիսիք են՝ երեխաների հանդեպ բռնությունը, նրանց շահագործումը, մանկապղծությունը, անչափահասներին սեռական կապերի մեջ ներքաշելը և, նույնիսկ, երեխաների վաճառքը:

Դաժան խաղեր

Բռնության վրա հիմնված խաղերը (ցանցային, բազմաօգտատիրական), արագորեն փոխարինում են «պասսիվ» դաժան ֆիլմերին: Բռնության վրա հիմնված խաղերի ազդեցությունը երիտասարդների վարքի վրա, բուռն վեճերի առարկա է: Առավել հայտնի խաղերը ցուցադրում են զենքի տարբեր տեսակներ (ինչպես իսկական, այնպես էլ հորինված), արյունահեղություն և համարվում են «սթրես հանելու» միջոց: Տարբեր հարթակների, ներառյալ Microsoft Xbox, Nintendo DS, Nintendo Wii, PC, Playstation, PSP համար ամենահանրաճանաչ խաղերը «հրաձգությունները» և այլ դաժան խաղերն են:

Հիմնախնդիրների լուծման տարբերակները

Համացանցում երեխաների պաշտպանության համատեքստում հիմնական բարդությունը, որի հետ բախվում են մանկավարժներն ու ծնողները, այն է, որ «թվայնացված սերունդը» ավելի շատ բան գիտի տեղեկատվական տեխնոլոգիաների մասին, միևնույն ժամանակ ավելի վատ է հասկանում դրանց հավանականա հետևանքները: Այդպիսի պայմաններում մեծ է հասակակիցների, ծնողների, մանկավարժների և ողջ հասարակության համագործակցությունը: Ամբողջ աշխարհում ծնողները, որոշումներ կայացնող անձինք և հասարակայնության ներկայացուցիչները աստիճանաբար ընդունում են վերը նշված հիմնախնդրի առկայությունը և տարբեր քայլեր են ձեռնարկում ուղղված «թվայնացված շրջակա միջավայրում» երեխաների պաշտպանությանը: Շահագրգիռ տարբեր կողմերի տեղեկացվածության մակարդակը բարձրացնելու համար Եվրախորհուրդն իրագործում է համացանցում անվտանգության հարցերով կենտրոնների (e-safety) համաեվրոպական ցանցի ստեղծմանն ուղղված InSafe նախագիծը: Այդ նախագծի շրջանակներում տարբեր լեզուներով նախապատրաստվել են մեծ թվով ուսումնական և տեղեկատվական նյութեր՝ ծնողների և մանկավարժների համար: Այդ բոլոր նյութերը մատչելի են բեռնելու և լայնորեն տարածելու համար: Լեհաստանի ԶԼՄ-երը պայքար սկսեցին համացանցում ահաբեկումների դեմ, որի արդյունքում երեխաների

համար ստեղծվեց համացանցում անվտանգության վերաբերյալ տեսահոլովակների սերիա և հեռակառավարելի ուսուցման դասընթաց:

Համացանցում անվտանգության վերաբերյալ ազգային մակարդակով առաջին նախաձեռնություններից է NetSafe նախագիծը, որը 1998 թ. իրականացվեց Նոր Զելանդիայում՝ նախարարությունների, բիզնեսի և ՀԼՄ-երի մասնակցությամբ:

Ազգային մակարդակով տեղեկատվաուսումնական քարոզարշավների ամենահաջողված մոդելներից մեկը համարվում է «Կիբեռաշխարհ» նախաձեռնությունը (Cyber-Peace Initiative): Այն ստեղծվել է Եգիպտոսում՝ Հանուն խաղաղության կանանց միջազգային շարժման հովանու ներքո, որի ղեկավարը Սյուզաննա Մուբարաքն էր: Ստեղծվեցին և ուսուցանվեցին համապատասխան նախագծերով կառավարման և անցկացման խանդավառ երիտասարդների խումբ, որը կոչվում էր «Net-Aman», ինչպես նաև մեկ այլ խումբ, որի կազմի մեջ էին մտնում ծնողները: Նրանք վերջին մի քանի տարվա ընթացքում գործընկերների, այդ թվում նաև Եգիպտոսի հեռահաղորդակցության նախարարության, Microsoft-ի տեղական ստորաբաժանման, ինչպես նաև միջազգային կազմակերպությունների (ChildNet International) հետ համատեղ տասնյակ երիտասարդների և նրանց ծնողների հետ մեծ աշխատանք են վարել ամբողջ երկրով մեկ: Բացի այդ, նրանք արաբերեն լեզվով նախապատրաստել էին տեղեկատվաուսումնական նյութերի մի քանի հավաքածու՝ երեխաների, նրանց ծնողների և մանկավարժների համար:

Հաշվի առնելով, որ 2009 թ. Եգիպտոսում կայանալու էր IGF հանդիպումը, կազմակերպիչները վստահ էին, որ այդ մոդելը լայն ճանաչում կգտնի և կկիրառվի նաև այլ երկրներում: Բացի երիտասարդներին, նրանց ծնողներին ու մանկավարժներին կրթելուց, անհրաժեշտ է բարձրացնել համացանցային անվտանգության ապահովման վերաբերյալ որոշումներ կայացնող անձանց՝ չինովնիկների, մասնավոր ընկերությունների աշխատակիցների, ոչ կառավարական կազմակերպությունների և ՀԼՄ-երի, ակադեմիական միությունների ներկայացուցիչների և «գիտահետազոտական կենտրոնների» որակավորումը: Միջազգային տարբեր կազմակերպություններ, այդ թվում նաև Եվրամիությունը, ՀՄՄ, «Կիբեռաշխարհը» և DiploFoundation-ը, քննարկում են այդպիսի ծրագրեր ստեղծելու հարցում համագործակցության հավանական մոդելները: Մոտ ապագայում անհրաժեշտ է նաև ուսումնական ծրագրերը բարեփոխել և դպրոցներում ուսուցման ընթացքում ընդգրկել այնպիսի հարցեր, ինչպիսիք են՝ անվտանգությունը համացանցում, անձնական տվյալների պահպանումը, անվտանգության ապահովումը, առցանց սեփական և օտարների հեղինակության հանդեպ ուշադրությունը, բարոյագիտությանը վերաբերող հարցերը, հանցավոր վարքի նկատմամբ վերաբերմունքը և այլն: Այդպիսի

մի շարք նախաձեռնություններ արդեն գոյություն ունեն: Դրանց թվում են՝ Cyber Smart!, iKeepSafe, i-Safe и NetSmartz:

Համացանցում երեխաների անվտանգության ապահովման անքակտելի բաղադրիչը ազգային և միջազգային իրավական ու քաղաքական մեխանիզմների համաձայնեցումն է: Վերջին օրինակներից է «Երեխաների համար անվտանգ համացանցի վերաբերյալ Պրահայի հռչակագրի» համաեվրոպական հաջողությունը, որն ընդունվել է 2009 թ. ապրիլին, ԵՄ նախարարների համաժողովում: ՀՄՄ-ն երեխաների առցանց պաշտպանության նախաձեռնությունը ընդգրկել է իր «Կիբեռանվտանգության ոլորտում համաշխարհային օրակարգի մեջ»: Բացի այդ, երեխաների պաշտպանությունն ընդգրկված է և ակտիվորեն քննարկվում է նաև միջազգային շատ ֆորումների օրակարգերում, ներառյալ IGF-ի, որի շրջանակներում գործառնում է երեխաների առցանց անվտանգության դինամիկ կոալիցիան:

Երեխաների պաշտպանության ոլորտում միջազգային համագործակցության հաջողված օրինակ է նաև վաղուց գոյություն ունեցող միջազգային «թեժ գծերը», որոնցից են՝

-երեխաների շահագործման վերաբերյալ նյութերը համացանցում տարածելու դեմ պայքարի նախագիծը (CIRCAMP), որի նախաձեռնողը Եվրամիության երկրների ոստիկանական ուժերի ղեկավարների աշխատանքային խումբն է.

-ոչ կառավարական այնպիսի կազմակերպությունների գործունեությունն ու պետական մարմինների հետ համագործակցությունը, ինչպիսիք են՝ Internet Watch Foundation, Perverted Justice Foundation, ICMEC, ECPAT, Save the Children, Internet Content Rating Association, Child Exploitation and Online Protection Centre.

-մասնավոր-պետական գործընկերությունները, որի վառ օրինակ է Նորվեգիայի ոստիկանության և Norway Telecom ընկերության միջև համագործակցությունը:

Ծանոթագրություններ

1.ԱՀԸ –ի (Առաջադեմ հեռահաղորդակցությունների ընկերակցություն) կանոնադրությունը ընդգրկում է հետևյալ դրույթները՝ բոլորի համար համացանց ներթափանցելու իրավունք, հավաքների և համագումարների արտահայտման ազատություն, գիտելիքների մատչելիություն, ուսուցման և ստեղծագործական աշխատանքում համագործակցություն, բաց կոդով ազատ ծրագրային ապահովման և այլ տեխնոլոգիաների մշակում, մասնավոր կյանքի պաշտպանություն, հետապնդումից պաշտպանություն, տվյալների գաղտնագրում, համացանցի կառավարում, գիտելիք, սեփական իրավունքների պաշտպանություն ու իրականացում: Լրացուցիչ տեղեկատվություն տես՝ http://www.apc.org/en/node/5677:

2. Առավել մանրամասն տեղեկատվություն տես՝ http://www.globalnetworkinitiative.org:

3.Համացանցային հասցեն՝ http://conventions.coe.int/treaty/EN/Treaties/html/005.htm

4. Մարդու իրավունքների և համացանցի վերաբերյալ Եվրախորհուրդն ընդունել է հետևյալ հիմնական հռչակագրերը՝ «Համացանցում հեռահաղորդակցության ազատության մասին հռչակագիր» (2003 թ. մայիսի 28), Տեղեկատվական հասարակությունում օրենքի գերակայության և մարդու իրավունքների մասին հռչակագիր (2005 թ. մայիսի 13):

5. Ավելի մանրամասն տեղեկատվության համար տես՝ http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FreedomOnTh eNet_FullReport.pdf:

6. Timothy Zick (1999). Congress, the Internet, and the intractable pornography problem: the Child Online Protection Act of 1998, Creighton Law Review, 32, pp. 1147, 1153, 1201

7. Համացանցում արգելված խաղերի հիմնախնդրի քննարկում, տես՝ Jenna F. Karadbil (2000), Note: Casinos of the next millennium: a look into the proposed ban on internet gambling, Arizona Journal of International and Comparative Law, 17, 413, 437-38:

8. Տես՝ «Համացանցը հսկողության ներքո» զեկույցը («Internet Under Surveillance»): Համացանցային հասցեն՝ http://www.rsf.org/rubrique.php3?id_rubrique=433.

9. Jonathan Zittrain and Benjamin Edelman, Documentation of Internet fi ltering worldwide (Open Net Initiative): http://cyber.law.harvard.edu/fi ltering/:

10. Չինաստանի իշխանությունները կիրառում են IP-հասցեների ուղեկապումը: Սաուդյան Արաբիայում համացանցային նյութերի զտումը պաշտոնապես իրականացվում է վստահված սպասարկուների համակարգի միջոցով: Լրացուցիչ տեղեկատվություն տես՝ http://www.isu.net.

sa/saudi-internet/contenet-fi ltring/fi ltring-mechanism.htm:

11. Տես՝ Electronic Frontiers, Australia, «Internet censorship in Australia» (20 December 2002), http://www.efa.org.au/Issues/Censor/cens1.html.

12. «Բովանդակության ընտրության համար համացանցային հարթակի» մասին լրացուցիչ տեղեկատվություն (Platform for Internet Content Selection, PICS), см.: http://www.w3.org/PICS/iacwcv2.

htm.

13. Վինգ Սերֆը, թեև մասնակցում էր փորձագետների խմբի աշխատանքներին, սակայն նա իր անհամաձայնությունն է հայտնել ամփոփիչ զեկույցի վերաբերյալ, որում, նրա խոսքերի համաձայն. «ուշադրության չեն արժանացվել առցանց զտումը կիրառելու հիմնախնդիրը և այդ գործողությունների համաշխարհային հետևանքները»: Աղբյուրը՝ «Welcome to the world wide web, passport, please?», New York Times, 15 March 2001 (համացանցային հասցեն՝ http://www.quova.com/page.php?id=33&coverage_id=86).

14. Akamai ընկերության ներկայացուցիչների խոսքերի համաձայն, նրա ծրագրային ապահովումը կարող է ստույգ, ընդհուպ փոստային ինդեքսը, որոշել օգտատիրոջ գտնվելու աշխարհագրական վայրը: Տեխնոլոգիապես մեծ ճշտությունն անհնար

է: Օգտատիրոջ հասցեի մասին տեղեկատվություն ստանալ չի կարելի IP հասցեի հիման վրա: Այդպիսի տեխնոլոգիաների առաջատար մատակարարներից մեկը՝ «Silicon Valleys Quova Inc կազմակերպությունը հայտարարում է, որ դեպքերի միայն 98 տոկոսում կարելի է որոշել այն երկիրը , որտեղ գտնվում է օգտատերը, իսկ քաղաքը կարելի է որոշել դեպքերի 85 տոկոսում: Անկախ հետազոտությունները այդպիսի ծրագրերի ստույգությունը գնահատում են InfoSplit, Digital Envoy, Netgeo և այլ ընկերությունների մատակարարման 70–0 % մակարդակով»: Տես՝ "Rise of internet borders prompts fears of web's future" by Arianna Eunjung Cha, Washington Post, January 4, 2002, p. E01:

15. Նյութի վերաբերյալ հրապարակումների ամփոփումը տես՝ http://searchenginewatch.com/sereport/article. php/2165031

16. Հրապարակվել է New Scientist ամսագրի համացանցային տարբերակում՝ http://www.newscientist. com/news/news.jsp?id=ns99992797

17. Տես՝ . Jonathan Zittrain and Benjamin Edelman, Localised Google search result exclusions: statement of issues and call for data (համացանցային հասցեն՝ http://cyber.law.harvard.edu/fi ltering/google/).

18. «Will all of us get our 15 minutes on a YouTube video?" by Lee Gomes. Th e Wall Street Journal. August 30, 2006 (համացանցային հասցեն՝ http://online.wsj.com/public/article/SB115689298168048904-5wWyrSwyn6RfVfz9NwLk774VUWc_20070829.html?mod=rss_free).

19. EU Information Society, «Safer internet action plan» (համացանցային հասցեն՝ http://europa. eu.int/information_society/programmes/iap/index_en.htm).

20. Տես՝ Church of Scientology censors net access for members (համացանցային հասցեն՝ http://www.xenu.net/archive/events/censorship).

21. Այս բաժնի համար արժեքավոր մեկնաբանություններ և գաղափարներ է արտահայտել Կատիտցա Ռոդրիգեսը (Katitza Rodriguez):

22. Քաղաքացիական իրավունքի համար ամերիկյան միության զեկույցը (American Civil Liberties Union): Jay Stanley (2004). Th e surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a) surveillance society (համացանցային հասցեն՝ http://www.aclu.org/FilesPDFs/surveillance_report.pdf):

23. «Հայրենասիրական գործողության» տեքստը տես՝ http://www.epic.org/privacy/terrorism/hr3162. html

24. Ընկերությունների կողմից անձնական տվյալների պահպանման առնչությամբ օգտատերերի վստահության հիմնախնդրի քննարկումը տես՝ Rick Whiting. Wary customers don't trust business to protect privacy, Information Week, August 19, 2002 (համացանցային հասցեն՝ http://www.informationweek.com/shared/printableArticle.jhtml?articleID=6503045).

25. Council of Europe, Convention for the protection of individuals with regard to the automatic processing of personal data, ETS No. 108 (համացանցային հասցեն՝ http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm).

26. Gramm-Leach-Bliley Act, Public Law (համացանցային հասցեն՝ http://frwebgate.access.gpo. gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106).

27. Children's Online Privacy Protection Act (համացանցային հասցեն՝ http://www.ftc.gov/ogc/coppa1.pdf U.S.C. §§ 6501-6505).

28. Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, § 264; Department of Health and Human Services, Standards for Privacy of Individually Identifi able Health Information; Proposed Rule, 64 Fed. Reg. 59917, (համացանցային հասցեն՝ http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html).

29. Galexia, the US Safe Harbour –Fact or Fiction?, 2008

30. Համացանցում բազմալեզվության մասին լրացուցիչ տեղեկություններ տես՝ Qusai AlShatti, Raquel Aquirre and Veronica Cretu. Multilingualism –the communication bridge.

DiploFoundation's Internet Governance Research Project, 2006/2007 (համացանցային հասցեն՝ http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.

edu/thina/txgetxdoc.asp?IDconv=3241).

31. Տես՝ http://en.wikipedia.org/wiki/English_in_computing#English_on_the_World_Wide_Web.

32. Համացանցի՝ որպես համաշխարհային հասարակական բարիքի մասին լրացուցիչ տեղեկատվություն տես՝ Seiiti Arata and Stephanie Psaila. Protection of Public Interest on the Internet.

DiploFoundation's Internet Governance Research Project, 2005/2006 (համացանցային հասցեն՝ http://www.diplomacy.edu/ig/Research/display.asp?Topic=Research%20Th emes %20II#Protection).

33. Այս բաժնի համար արժեքավոր մեկնաբանություններ և գաղափարներ է տրամադրել Խորխե Պլանոն (Jorge Plano):

34. Տես՝ http://www.hrea.org/index.php?base_id=152

35. Տես՝ http://www.un.org/disabilities/

36. Տես՝ http://www.intgovforum.org/cms/index.php/dynamic-coalitions/80-accessibilityand-

disability and http://www.itu.int/themes/accessibility/dc/

37. Տես՝ http://www.isocdisab.org

38. Տես՝ http://www.w3.org/TR/WCAG10/

39. Տես՝ http://www.isoc.org/briefi ngs/002/isocbriefi ng02.txt

40. Այս տեքստը կազմել էր Վլադիմիր Ռադունովիչը (Vladimir Radunovic)՝ համացանցում անվտանգության և կիբեռանվտանգության վերաբերյալ դասընթացի համար: DiploFoundation (Advanced Course on Cybersecurity and Internet Safety, Internet Governance Capacity Building Program).

Բաժին 7

Համացանցի կառավարման գործընթացի մասնակիցները

Համացանցի կառավարման գործընթացի մասնակիցները

Համացանցի կառավարման բնորոշ հատկանիշը միշտ եղել է այն, որ նրանում տարբեր շահագրգիռ կողմեր են մասնակցել: Այդպիսի «բազմակողմանիությունը» միանգամայն բնական է, քանի որ համացանցի գործառույթների ստեղծման ու աջակցման գործում հիմնական մասնակցությունը ոչ պետական սուբյեկտներն են ունեցել: Քաղաքացիական հասարակությունը և, հատկապես, ակադեմիական շրջանակները հիմնական դեր են կատարել համացանցի ձևավորման գործում, ներառյալ արձանագրությունների մշակումը, բովանդակության և առցանց միությունների ստեղծումը: Աճող պահանջարկին ի պատասխան բիզնեսի ջանքերով ստեղծվել է տեխնոլոգիական ենթակառուցվածք՝ համակարգիչներ, ցանցեր, ծրագրային ապահովում: Իսկ կառավարությունները համացանցի կառավարման ասպարեզում նորելուկներն էին[1]: Համացանցի կառավարման վերաբերյալ բանակցությունների և համաշխարհային այլ բանակցությունների միջև, օրինակ՝ շրջակա միջավայրի պահպանման բնագավառում, հիմնական տարբերությունն այն է, որ եթե այլ դեպքերում միջկառավարական կարգերն աստիճանաբար «բացվում էին» ոչ պետական մասնակիցների համար, ապա համացանցի կառավարման վերաբերյալ բանակցություններում կառավարությունները ստիպված էին ընդգրկվել արդեն գոյություն ունեցող ոչ կառավարական կարգում, որի կենտրոնը ICANN-ն էր:

Համացանցի կառավարումը մոտեցում է «փոփոխական երկրաչափությամբ»

Համացանցի կառավարումը պահանջում է տարբեր շահագրգիռ կողմերի մասնակցություն, որոնք զանազանվում են շատ պարամետրերով, ներառյալ միջազգային իրավաունակությունը, համացանցի կառավարման կոնկրետ հարցերի հանդեպ շահագրգռվածությունը և փորձագիտական գիտելիքների առկայությունը: Այդպիսի բազմազանությունը կարելի է միաձուլել համացանցի կառավարման մեկ միասնական մոդելում՝ կիրառելով «փոփոխական երկրաչափության» մոտեցումը: Այս մոտեցումը, որը հաշվի է առնում համացանցի կառավարման հարցերի լուծման ոլորտում շահագրգիռ կողմերի հնարավորություններն ու գերակայությունները, իր արտացոլումն է գտել WSIS սկզբունքների հռչակագրի 49-րդ հոդվածում, որն էլ հիմնական շահագրգիռ կողմերի համար սահմանում է հետևյալ դերերը՝[3]

-պետություններ. «քաղաքական լիազորություններ համացանցի հետ կապված պետական քաղաքականության հարցերով» (միջազգային տեսակետները ներառյալ)

-մասնավոր սեկտոր. «համացանցի զարգացումը ինչպես տեխնիկական, այնպես էլ տնտեսական բնագավառում»,

- քաղաքացիական հասարակություն. «համացանցին վերաբերող հարցերում կարևոր դեր, հատկապես համայնքներում»,

- միջկառավարական կազմակերպություններ՝ «համացանցի հետ կապված պետական քաղաքականության հարցերի կոորդինացումը»,

-միջազգային կազմակերպություններ՝ «համացանցին վերաբերող տեխնիկական ստանդարտների և համապատասխան քաղաքականության մշակում»:

Համացանցի կառավարման հարցերը, երբ հասան համաշխարհային մակարդակի, քաղաքականության բազմակողմ մոդելի ստեղծման միջոցով այդ երկու կարգերը (ոչ կառավարական և ավանդական դիվանագիտական) ինտեգրացնելու անհրաժեշտություն առաջացավ: Այդ ուղղությամբ առաջին հաջողված փորձը համացանցի կառավարման աշխատանքային խումբն էր (WGIG), որն ստեղծվել էր WSIS-ի (2003–2005) նախապատրաստման գործընթացում: WGIG-ը փորձագիտական, խորհրդատվական խումբ է, սակայն որոշումներ կայացնող կառույց չէ[2]: Այն չի կազմել ՄԱԿ-ի պաշտոնական փաստաթղթեր, սակայն ազդեցություն է գործել WSIS-ի ընթացքում համացանցի կառավարման բանակցությունների վրա: WGIG-ը ստեղծվել է ICANN-ին աջակցող կառավարությունների միջև փախզիջումների արդյունքում, որոնք պաշտոնապես թույլատրել են բազմակողմ դիվանագիտական օրակարգում համացանցի կառավարման հարցերի ի հայտ գալը, ինչպես նաև այլ, հիմնականում, զարգացող երկրների կառավարությունների փոխզիջումների, որոնք համաձայնվել են գործընթացին ոչ կառավարական սուբյեկտների մասնակցությանը: Այդ փոխզիջման արդյունքը WGIG-ի հաջողությունն էր: WSIS-ի ավարտից հետո համացանցի կառավարումը մտնում է համաշխարհային օրակարգում որպես համացանցի օգտագործումը կառավարող ֆորում, որի չորրորդ հանդիպումը տեղի է ունեցել 2009 թ. նոյեմբերին, Շարմ էշ Շեյխում (Եգիպտոսում): Առաջին հնդիպումն անցկացվել է Աթենքում (Հունաստան) 2006 թ., երկրորդը՝ Ռիո դե Ժանեյրոյում (Բրազիլիա), 2007 թ. երրորդը՝ Հայդարաբադում (Հնդկաստան), 2008 թ.: IGF-ում մասնակցելու կռուցվածքը

նման է WGIG-ին. այդ կառուցվածքները միջազգային մակարդակում բազմակողմ գործընկերութան օրինակներ են մտում:
Այս գլխում քննարկվում է համացանցի կառավարման գործընթացում հիմնական շահագրգիռ կողմերի դերի մասին: Մենք կսկսենք WSIS և WGIG գործընթացում պաշտոնապես ճանաչված սուբյեկտներից, ներառյալ կառավարությունները, միջազգային կազմակերպությունները, քաղաքացիական հասարակությունն ու բիզնեսը: Համառոտ կքննարկենք նաև կարևորագույն այլ մասնակիցների, առաջին հերթին՝ համացանցային միութունների և ICANN-ի դերը:

Պետություն

2003 թ. համացանցի կառավարման հարցերը քաղաքական օրակարգում հայտնվելուց հետո, վերջին վեց տարիները շատ պետությունների համար ուսման տարիներ էին: Համացանցի կառավարման հարցերի լուծմանը նույնիսկ խոշոր եւ հարուստ երկրների մասնակցությունը կապված է բազմաթիվ բարդությունների հետ, այդ թվում նաև համացանցի կառավարման միջկարգապահական բնույթի (տեխնոլոգիական, սոցիալական, տնտեսական տեսանկյունները) և այդ գործընթացին մասնակցող սուբյեկտների մեծ տարբերությունների պատճառով: Շատ պետություններ ստիպված էին իրենց համար այս նոր հարցը ընկալել «ոտքի վրա»՝ ուսուցանել չինովնիկներին, քաղաքականություն մշակել և ակտիվորեն մասնակցել համացանցի կառավարման վերաբերյալ տարբեր ֆորումների: Այս գլխում համացանցի կառավարման բնագավառի հիմնախնդիրները կքննարկենք պետությունների տեսանկյունից:

Կոորդինացում՝ պետության մակարդակով

WSIS գործընթացի սկզբում՝ 2003 թ. շատ երկրներում համացանցի կառավարման հարցերով սովորաբար զբաղվում էին «տեխնիկական» այն նախարարությունները, որոնք պատասխանատու էին Հեռահաղորդակցության միջազգային միության (ՀՄՄ) հետ հարաբերությունների համար: Աստիճանաբար գիտակցելով, որ համացանցի կառավարումը միայն «լարերն ու մալուխը» չէ, կառավարությունները դրանում ընդգրկեցին նաև այլ նախարարությունների ներկայացուցիչներին, օրինակ՝ մշակույթի, ԶԼՄ-երի, արդարադատության:
Համացանցի կառավարման հարցերի բազմազանությունը պայմանավորված է նաեւ այն բանով, որ դրանցով զբաղվում էին տարբեր սուբյեկտներ, ինչպիսիք են՝ ICANN-ը եւ տեխնիկական ստանդարտացման կազմակերպությունները: Շատ պետությունների համար հիմնական բարդությունը այնպիսի ռազմավարության մշակումն է, որն ուղղված է համացանցի կառավարման հարցերի լուծման համար անհրաժեշտ գիտելիքներին տիրապետող ոչ պետական հիմնարկությունների

«Հեռագրային աշխարհառազմավարություն» և քաղաքական (ան)համաձայնություն

Անգլիա-ֆրանսիական միությունը (Անտանտա) կազմավորվել է 1904 թ.: Սակայն Ֆրանսիայի հեռագրային նախարարությունը չհետևեց երկրի ընդհանուր քաղաքական ուղուն՝ սերտ համագործակցություն հաստատելով Գերմանիայի հետ: Դրա հիմնական նպատակը համաշխարհային «հեռագրային աշխարհառազմավարության» մեջ Բրիտանիայի գերիշխանության նվազեցումն էր՝ ի հաշիվ հեռագրային մալուխների անցկացման գործում Գերմանիայի հետ համագործակցության: Ֆրանսիացի պատմաբան Շառլ Լեզաժը քաղաքական այդ (ան)համաձայնությունը հետևյալ կերպ է մեկնաբանել. «Իմ կարծիքով, ֆրանսիական դիվանագիտության ընդհանուր սկզբունքների և հեռագրության ոլորտում գործողությունների միջև երկարատև հակասությունները հետևանք են այն բանի, որ այդ երկրում յուրաքանչյուր նախարարություն իր արտաքին քաղաքականությունն ունի: Մի քաղաքականություն է վարում արտաքին գործերի նախարարությունը, մեկ այլ քաղաքականություն՝ ֆինանսների նախարարությունը... Փոստի և հեռագրության վարչությունը նույնպես ժամանակ առ ժամանակ իր արտաքին քաղաքականությունն է վարում և ստացվեց այնպես, որ վերջին տարիներին Անգլիայի հանդեպ թշնամաբար տրամադրված չլինելով հանդերձ, բացահայտ հակվածություն ցուցաբերեց դեպի Գերմանիան»[5]:

աջակցության կոորդինացմանը ու ձեռքբերմանը, օրինակ՝ համալսարաններ, մասնավոր ընկերություններ, ոչ կառավարական կազմակերպություններ: WSIS-ի ընթացքում միջին և խոշոր պետություններից շատերին հաջողվեց ձեռք բերել անհրաժեշտ ինստիտուցիոնալ ներուժ՝ համացանցի կառավարման վերաբերյալ համաշխարհային բանակցությունների մոնիտորինգի համար: Դրանցից մի քանիսը, ինչպես, օրինակ՝ Բրազիլիան, ստեղծեցին նորարարական ազգային կառույցներ, որոնք հետևում էին համացանցի կառավարմանը վերաբերող բանավեճերին[4]:

Քաղաքական ուղիների համաձայնեցումը

Հաշվի առնելով համացանցի կառավարման բազմամասնագիտական բնույթը և քննարկման վայրերի (կայքերի) բազմազանության ու մասնակիցների բարձր մակարդակը, այս բնագավառում քաղաքական ուղիների համաձայնեցման հասնելը շատ բարդ է: Սա կառավարման հիմնախնդիր է, որը կառավարություններից պահանջում է քաղաքականության մշակման գործընթացի համակարգման ճկուն մոտեցում, ներառյալ հորիզոնական հեռահաղորդակցությունը՝ տարբեր նախարարությունների, բիզնես շրջանակների և այլ սուբյեկտների միջև: Ավանդական կառավարման կառույցը, որ ստեղծված է հիերարխիկ սկզբունքով, կարող է խոչընդոտ լինել այդպիսի ճկուն համակարգման համար: Բացի զուտ կառավարման բարդություններից, քաղաքական ուղիները համաձայնեցնելու հնարավորությունը հաճախ սահմանափակվում է քաղաքական շահերի մրցակցության առկայությամբ: Սա արդարացի է հատկապես զարգացած և բազմազան համացանցային տնտեսություն ունեցող երկրների համար: Բերենք ցանցային չեզոքության հարցի վերաբերյալ վերջերս տեղի ունեցած բանավեճերի օրինակը, որոնց ընթացքում ԱՄՆ կառավարությունը ստիպված էր հավասարակշռություն մտցնել համացանցային ընկերություններից ցանցային չեզոքության կողմնակիցների (Google, Yahoo!)

և հեռահաղորդակցային կապի-զվարճությունների սեկտորի միջև (Verizon, AT&T, հոլիվուդյան լոբբի), որը ցանցային չեզոքությունը դիտարկում է որպես խոչընդոտ ավելի արագ համացանց ստեղծելու ճանապարհին՝ մուլտիմեդիա նյութերի օգտատերերին մատակարարելու համար: Տարբեր մեդիաների միացումը ևս մի խթան է քաղաքական ուղիների համաձայնեցմանը հասնելու: Կարգավորման տարբեր ոլորտները (հեռահաղորդակցությունները, հեռուստա և ռադիոհաղորդման ցանցերը) ստիպված են «ընդհանուր հայտարարի» գալու, որպեսզի հետ չմնան տեխնոլոգիաների մերձեցման գործընթացից:

Ժնևի մշտական առաքելությունների կարևորությունը

Շատ պետություններ Ժնևում տեղի ունեցող մշտական առաքելություններում WSIS և ամբողջությամբ վերցրած համացանցի կառավարման գործընթացի կարևոր, եթե չասենք առանցքային խաղացողներն էին: Ակտիվ գործունեության մեծ մասը տեղի էր ունենում Ժնևում, որտեղ տեղակայված է գործընթացում հիմնական դեր կատարող ՀՄՄ կենտրոնակայանը: WSIS-ի առաջին գագաթաժողովը տեղի է ունեցել 2003 թ. Ժնևում ու դրանից հետո, բացառությամբ մեկի, բոլոր նախապատրաստական հանդիպումները անց էին կացվում այնտեղ, որի շնորհիվ Ժնևի մշտական առաքելությունները ներգրավվում էին գործընթացի մեջ:

Ներկայում IGF քարտուղարությունը տեղակայված է Ժնևում, որտեղ էլ անցկացվում են IGF-ի նախապատրաստական բոլոր հանդիպումները: Զարգացած խոշոր պետությունների համար մշտական ներկայացուցչությունները կազմակերպությունների եւ անհատների լայն ցանցի մի մասն էին, որ մասնակցում էին WSIS-ին և համացանցի կառավարման գործընթացին: Իսկ զարգացող և փոքր պետությունների համար մշտական ներկայացուցչությունները գործընթացի հիմնական, երբեմն նույնիսկ միակ մասնակիցներն էին: WSIS-ի թղթապանակն ավելացել է սովորաբար, զարգացող երկրների փոքր, առանց այն էլ ծանրաբեռնված ներկայացուցչությունների օրակարգում: Երբեմն նույն դիվանագետը ստիպված էր լինում WSIS-ի հետ կապված խնդիրները կատարել այլ ոլորտների առաջադրած պարտականությունների հետ, ինչպիսիք են՝ մարդու իրավունքները, առողջապահությունը, առևտուրը, աշխատանքի ապահովումը:

Համացանցի կառավարման գործընթացի «դիվանագիտականացումը»

WSIS-ի ընթացքում կառավարությունների դիրքորոշումների համար կարևոր էր նաև այն, որ այդ գագաթաժողովը համացանցը ընդգրկել էր համաշխարհային հարցերի օրակարգում: Մինչ WSIS-ը, համացանցը քննարկվում էր առավելապես ոչ կառավարական շրջանակներում կամ ներքաղաքական մակարդակով: Համացանցի քաղաքական տեսակետների «դիվանագիտացումը» տարբեր արձագանքներ առաջ բերեց: The Economist ամսագրի տեխնոլոգիական մեկնաբան Քեննեթ Նիլ

Կուկյերը ընդգծել է համացանցի կառավարման վերաբերյալ բանավեճերի «դիվանագիտացման» բացասական տեսակետը. «... Նախքան ՄԱԿ-ի պաշտոնական գագաթաժողովը հիմնախնդրի քննարկման մակարդակի բարձրացումը, բնականաբար, բարձրացնում է այդ թեմայի կարևորությունը կառավարությունների շրջանակներում: Արդյունքում տեղեկատվական հասարակության թեման, որով (ինչպես որ գիտատեխնիկական քաղաքականության հարցերով) զբաղվում էին նվազ քաղաքականացված և կառավարության ավելի քիչ աչքի ընկնող կառույցները, փոխանցվում է արտաքին գործերի նախարարություններին և փորձառու դիվանագետներին, ովքեր ավելի շատ սովոր էին ուժային քաղաքականությանը և քիչ էին տեղեկացված տեխնիկական տեսանկյունների ու համացանցին ներհատուկ համագործակցության ու փոխկախվածության մասին»[6]:
Գործընթացի դիվանագիտացումը WSIS-ի ընթացքում տեղի ունեցող քննարկումների համար ունեցավ նաև որոշակի դրական հետևանքներ: Օրինակ՝ դիվանագետներն անաչառ մեկնաբանություններ արեցին համացանցում անունների և համարների շնորհման ընկերությունների հետ կապված վաղեմի այնպիսի հիմնախնդիրների վերաբերյալ, ինչպիսիք են՝ դոմենային անունները, IP հասցեները և հիմնական սպասարկուները: Դիվանագետների ներդրումը հատկապես նկատելի էր WGIG բանավեճերում: WGIG-ի դիվանագետ առաջնորդները (նախագահ Նիթին Դեսային և գործադիր տնօրեն Մարկուս Կումմերը) ստեղծել էին մասնակցության մթնոլորտ, որում խմբի անդամների միջև տարբերությունները, ներառյալ տեխնիկական միությունների ներկայացուցիչները, չէին ուղեփակել գործընթացը: WGIG-ի աշխատանքի արդյունքն ամփոփիչ հաշվետվությունն էր, որում նշվում էին հակասությունները, սակայն առաջարկվում էր նաև լուծում՝ համացանցի օգտագործման կառավարման համաժողովի ձևով կազմակերպված հետագա քննարկումների գործընթացի վերաբերյալ:

ԱՄՆ կառավարության դիրքորոշումը

Համացանցը մշակվել է մի նախագծի շրջանակներում, որը ֆինանսավորում էր ԱՄՆ կառավարությունը: Համաշխարհային ցանցի ի հայտ գալուց ի վեր մինչ օրս ԱՄՆ կառավարութունը մասնակցել է համացանցի կառավարմանը տարբեր նախարարությունների և գերատեսչությունների միջոցով. նախ՝ պաշտպանության նախարարության, այնուհետև Գիտության ազգային հիմնադրամի, և վերջապես, արևտրի նախարարության միջոցով: Համացանցի զարգացման համար իրավակարգավորիչ բազա ստեղծելու գործում կարևոր դեր է կատարել Կապի դաշնային հանձնաժողովը: ԱՄՆ կառավարության մասնակցության բնորոշ գծերից մեկը չմիջամտելու քաղաքականությունն էր, որը սովորաբար կոչվում էր «հեռավոր խնամակալ»: Ամերիկյան իշխանությունները միայն ընդհանուր շրջանակներ տվեցին, համացանցի կառավարման իրականացումը թողնելով նրանց, ովքեր դրա հետ անմիջականորեն աշխատում են, առաջին հերթին՝ համացանցային միություններին: Սակայն որոշ դեպքերում ԱՄՆ

կառավարությունը այդ գործընթացին միջամտել է բացահայտորեն, օրինակ՝ 1990-ականներին, երբ CORE[1] նախագծի շրջանակներում հիմնական սպասարկուներն ու համացանցի գլխավոր ռեսուրսների կառավարումը կարող էին ԱՄՆ-ից տեղափոխվել Ժնեւ: Այդ գործընթացը դադարեցվեց համացանցի պատմության մեջ հիշարժան ծայրահեղ միջոցով՝ ՀՄՄ գլխավոր քարտուղարին ուղղված ԱՄՆ պետքարտուղար Մադլեն Օլբրայթի դիվանագիտական նոտայով[7]: CORE նախաձեռնության դադարեցմանը զուգահեռ, ԱՄՆ կառավարությունը խորհրդատվություններ էր սկսել, որի արդյունքում ստեղծվեց ICANN-ը: Դրա ստեղծման պահից ԱՄՆ կառավարությունը հայտարարեց, որ մտադիր է դադարեցնել ICANN-ի կառավարումն միայն այն ժամանակ, երբ այդ կազմակերպությունը կդառնա ինստիտուցիոնալ և գործառույթներով կայուն: Այդ գործընթացը սկսվեց 2009 թ. հոկտեմբերին, երբ ԱՄՆ առևտրի նախարարությունը ստորագրեց «Պարտականությունների հաստատումը»: Այդ փաստաթղթի համաձայն, ICANN-ը կդառնա անկախ կազմակերպություն:
Առևտրի նախարարության և ICANN-ի միջև հատուկ հարաբերությունների մեկ այլ տարրը, այսպես կոչված, IANA[2]-ի վերաբերյալ համաձայնագիրը վերանայվելու է 2011 թ.: WSIS-ի ընթացքում համաշխարհային մակարդակով ԱՄՆ-ն հանդես է եկել ICANN-ի գործառույթները միջկառավարական կառույցի հանձնելու հավանականության դեմ: Սակայն հենց այդ ժամանակ ամերիկյան կառավարությունը առաջին քայլերն էր անում ICANN-ի ինտերնացիոնալացմանն ուղղված, ընդունելով, որ պետությունների կառավարություններն իրավունք ունեն համապատասխան դոմենային անունների և համաձայնելով շարունակել միջազգային քննարկումները IGF ստեղծման ձևով:

*[1] **CORE - ոչ կառավարական կազմակերպություն, դոմենային անուններն արձանագրողների ընկերակցություն (http://www.corenic.org/):***
*[2] **Internet Assigned Numbers Authority (Համացանցում համարներ շնորհող վարչություն)՝ ICANN-ի վերահսկման ենթակա կառույց, որը զբաղվում է դոմենային անունների, IP հասցեների և համացանցային արձանագրությունների հետ կապված տեխնիկական առանձին հարցեր լուծելով (http://www.iana.org):***

Այլ պետությունների դիրքորոշումը

Համացանցի կառավարման քաղաքական սպեկտրը սկսել է ձևավորվել վերջերս, քանի որ տարբեր երկրների կառավարությունները ձևավորել են իրենց դիրքորոշումները: Ծայրահեղ տեսակետներից մեկի համաձայն, համացանցը պետք է կառավարի այնպիսի միջկառավարական կազմակերպություն, ինչպիսին ՀՄՄ-ն է: Սկզբում այսպիսին էր զարգացող երկրների դիրքորոշումը: ՀՄՄ դերի ամրապնդման ամենաակտիվ կողմնակիցներն էին Չինաստանը, Իրանը, Ռուսաստանը և Բրազիլիան: Որոշ զարգացող երկրներ առաջարկում էին ՀՄՄ-ի փոխարեն ստեղծել միջազգային նոր կազմակերպություն («Համացանցի միջազգային

կազմակերպություն»), նույնիսկ միջազգային նոր պայմանագրի հիման վրա: Մյուս երկրները ընդգծում էին, որ համացանցը պետք է կառավարի նոր տիպի կազմակերպություն, որը կընդգրկի տարբեր շահագրգիռ կողմերի: Քաղաքական սպեկտրի կենտրոնում գտնվում են այնպիսի երկրներ, որոնք կողմնակից են ICANN-ի համար տեխնիկական գործառույթները պահպանելու և միջազգային այնպիսի նոր կառույց ստեղծելու, որը կվերահսկի քաղաքական տեսակետները: Աստիճանաբար այսպիսի դիրքորոշում ընդունեց Եվրամիությունը: Եվ, վերջապես, սպեկտրի մյուս ծայրին է գտնվում ԱՄՆ-ն, որը պնդում է, որ ICANN-ի վրա հիմնված ներկա կարգը փոփոխելու կարիք չկա: Կանադան, Ավստրալիան և Նոր Զելանդիան նույնպիսի կարծիք հայտնեցին, միևնույն ժամանակ հանդես գալով որպես ICANN-ի ինտերնացիոնալիզացման կողմնակից: Այս պետությունները ԵՄ-ի, Շվեյցարիայի և մի քանի զարգացող երկրների հետ մասին մեծ դեր խաղացին WSIS շրջանակներում համացանցի կառավարման հարցում փոխզիջումային որոշումների հասնելու գործում:

Փոքր պետությունների դիրքորոշումը

Համացանցի կառավարման գործընթացում գործունեության դինամիկան և հարցերի բարդությունը ոչ մեծ, հատկապես զարգացող պետություններին թույլ չէին տալիս հետևել տեղի ունեցող իրադարձություններին, առավել ևս գործընթացի վրա որևէ նշանակալի ազդեցություն ունենալ: Եվ արդյունքում փոքր պետություններից շատերը համացանցի կառավարման հարցում աջակցեցին «մեկ պատուհանի» սկզբունքին8: Զարգացող երկրների սահմանափակ ներուժը և օրակարգի կետերի քանակը (ինչպես տվյալ երկրում, այնպես էլ նրա դիվանագիտական ներկայացուցչություններում) հիմնական խոչընդոտն են՝ համացանցի կառավարման գործընթացում նրանց լիարժեք մասնակցության համար: Այս բնագավառում ներուժ զարգացնելու անհրաժեշտությունը WSIS տեղեկատվական հասարակության համար թունիսյան ծրագրում ճանաչվել է որպես առաջնահերթություն:

Բիզնես[9]

1998 թ. երբ ստեղծվեց ICANN-ը, ըստ բիզնես միությունների, գլխավոր հիմնախնդիրներից մեկը ապրանքանիշերի պահպանությունն էր: Շատ ընկերություններ բախվեցին կիբեռսքվոթինգի հիմնախնդրին և այնպիսի մարդկանց հետ, ովքեր չարաշահում էին իրենց ապրանքանիշերի օգտագործումը և հասցրել էին առաջինը գրանցել համապատասխան դոմենային անվանումները: ICANN-ի ստեղծման գործընթացում գործարար շրջանակները ապրանքանիշերի պաշտպանությունը հստակ նշել էին որպես առաջնահերթություն, հետևաբար, այդ կազմակերպությունն ի հայտ գալով, անմիջապես զբաղվեց ապրանքանիշերի պաշտպանության հարցերով[10]: Ներկայում համացանցի ծավալման համապատասխան,

աճել է նաև բիզնեսի հետաքրքրությունը համաշխարհային ցանցի կառավարման հանդեպ: Այս տեսակետից ընկերությունները կարելի է բաժանել հետևյալ հիմնական խմբերի. դոմենային անուններով զբաղվող ընկերություններ, համացանցային ծառայություններ մատակարարողներ, հեռահաղորդակցային կապի ընկերություններ, ծրագրային ապահովման երևակիչներ և համացանցի համար կոնտենտ արտադրող ընկերություններ: Դոմենային անուններով զբաղվող ընկերությունները ընդգրկում են տարբեր մակարդակների գրանցողների և գրանցավայրեր, որոնք վաճառում են դոմենային անուններ համացանցում (օրինակ՝ .com, .edu): Այդ շարքում հիմնական դեր խաղացողներից են VeriSign и Affi lias ընկերությունները: Դրանց գործունեության վրա անմիջականորեն ազդում են ICANN-ի ընդունած քաղաքական որոշումներն այնպիսի ոլորտներում, ինչպիսիք են բարձր մակարդակի նոր դոմենների ստեղծումը և վեճերի լուծումը: Այդ պատճառով այս ընկերությունները շահագրգռված են ICANN-ում քաղաքականության մշակման գործընթացով: Նրանք մասնակցել են նաև համացանցի կառավարման ավելի լայնածավալ գործընթացի (WSIS, WGIG, IGF), որպեսզի նվազեցնեն այլ մասնակիցների, հատկապես կառավարությունների և միջազգային կազմակերպությունների կողմից ICANN-ի գործառույթների բռնագրավման վտանգը:

Ապրանքանիշերի վերաբերյալ մանրամասն բաժին 3-ում

Համացանցային ծառայությունների մատակարարներն (պրովայդերներ) այն ընկերություններն ու կազմակերպություններն են, որոնց օգնությամբ վերջին օգտատերերը ստանում են համացանցի հասանելիության իրավունք: Քանի որ մատակարարները ցանցում աշխատելիս գլխավոր միջնորդներն են համարվում, ապա դրանք առանձնահատուկ կարևորություն ունեն համացանցի կառավարման տեսակետից: Այդ գործընթացում դրանց հիմնական մասնակցությունը տեղի է ունենում ազգային մակարդակով՝ որպես կառավարության մարմինների և գերատեսչությունների հետ համագործակցություն: Համաշխարհային մակարդակով որոշ մատակարարներ, հատկապես ԱՄՆ-ից և Եվրոպայից, ակտիվորեն մասնակցում էին WSIS/WGIG/IGF-ին և՛ անհատապես, և՛ միջնորդավորված՝ Միջազգային առևտրային պալատի, ազգային, տարածաշրջանային և ճյուղային գործարար կազմակերպությունների կողմից, ինչպիսիք են, օրինակ՝ Հեռահաղորդակցային կապի օպերատորների եվրոպական ընկերակցությունը (ETNO), Տեղեկատվական տեխնոլոգիաների ամերիկյան

Միջազգային առևտրային պալատ (ՄԱՊ)

Միջազգային առևտրային պալատը (ՄԱՊ) իրեն դրսևորել է որպես գործարար շրջանակների առանցքային ներկայացուցիչներից մեկը համացանցի կառավարման համաշխարհային գործընթացներում: ՄԱՊ-ը ակտիվորեն մասնակցել է WGIG-ի և WSIS-ի վաղ շրջանի բանակցություններին ու շարունակում է ակտիվ ներդրում ունենալ IGF գործընթացում:

ընկերակցությունը (ITAA) և այլն:
Հեռահաղորդակցային ընկերություններն ապահովում են համացանցային թրաֆիկի փոխանցումը և սպասարկում են համացանցային ենթակառուցվածքները: Այդ հատվածում հիմնական դեր խաղացողներից են այնպիսի ընկերություններն, ինչպիսիք են Verizon-ը և AT&T-ն:
Հեռահաղորդակցային ընկերությունները ՀՄՄ-ի միջոցով ավանդաբար մասնակցում էին էլեկտրակապի բնագավառում միջազգային քաղաքականության մշակմանը: Նրանք ավելի ու ավելի ակտիվորեն են ներգրավվում ICANN-ի և IGF-ի գործունեության մեջ: Համացանցի կառավարման տեսանկյունից նրանք հիմնականում շահագրգռված են բիզնեսի համար բարենպաստ միջավայր ապահովել, որը թույլ կտա զարգացնել համացանցի հեռահաղորդակցային ենթակառուցվածքը:

Համացանցային ծառայությունների մատակարարների վերաբերյալ մանրամասն բաժին 2-ում

Ծրագրային ապահովում արտադրող ընկերությունները, ինչպիսիք են՝ Microsoft-ը, Adobe-ը և Oracle-ը, հիմնականում մասնակցում են ստանդարտացման գծով տարբեր կազմակերպությունների գործունեությանը (W3C, IETF): WSIS-ի գործընթացի վաղ փուլերում նրանց հիմնական մտահոգությունը համացանցում մտավոր սեփականության իրավունքների մասին քննարկումներ սկսելու հնարավորությունն էր: Ինչպես արտահայտվել է այդ սեկտորի ներկայացուցիչներից մեկը, նրանց նպատակն էր «վթարների մասին նախազգուշացնելը»: Երբ հայտնի դարձավ, որ WSIS-ը չի զբաղվելու մտավոր սեփականության հարցերով, նվազեց այդ գործին մասնակցելու ԾԱ արտադրողների հետաքրքրությունը: Այդ միտումը շարունակվեց նաև WSIS-ից հետո:
Մասնակիցների վերջին խումբը, որ նշվում է որպես «կոնտենտ արտադրող ընկերություններ», ընդգրկում է համացանցի հիմնական ապրանքանիշերը, ինչպիսիք են՝ Google-ը, Yahoo!-ն և Facebook-ը: Ընկերությունների այս խումբը ավելի ու ավելի կարևորվում է Վեբ 2.0 ծառայությունների զարգացմանը զուգընթաց: Դրանց առաջնահերթությունները սերտորեն կապված են համացանցի կառավարման տարբեր հիմնախնդիրների, մասնավորապես, մտավոր սեփականության, գաղտնիության և կիբեռանվտանգության պահպանման հետ, իսկ համացանցի կառավարման գործընթացում նրանց մասնակցությունը դառնում է ավելի նկատելի:

Մտավոր սեփականության իրավունքների մասին մանրամասն բաժին 3-ում

Քաղաքացիական հասարակություն

Քաղաքացիական հասարակությունը միշտ եղել է համացանցի կառավարման գործում տարբեր մասնակիցներ ներգրավելու ամենաակտիվ կողմնակիցը: Նախորդ բազմակողմ ֆորումներին քաղաքացիական հասարակության մասնակցությունը քննադատելու համար առիթը ներկայացուցիչների միջև պատշաճ համակարգման բացակայությունն էր և տարբեր, երբեմն հակասական դիրքորոշումների առատությունը:

Սակայն WSIS գործընթացում քաղաքացիական հասարակության ներկայացուցիչները կարողացան հաղթահարել այդ սեկտորին հատուկ բարդությունն ու բազմազանությունը՝ հիմնվելով կազմակերպչական մի շարք ձևերի, այդ թվում՝ Քաղաքացիական հասարակության բյուրոյի (Civil Society Bureau), Քաղաքացիական հասարակության պլենումի (Civil Society Plenary) և թեմատիկ խմբերի վրա: Բախվելով պաշտոնական գործընթացի վրա ազդելու իրենց սահմանափակ հնարավորություններին, քաղաքացիական հասարակության խմբերը մշակել են «երկուղի» մոտեցում: Ոչ կառավարական կազմակերպությունները շարունակում էին ներկա գտնվել պաշտոնական գործընթացում՝ օգտագործելով եղած հնարավորությունները կառավարությունների լոբբինգի և մասնակցության համար: Դրան զուգահեռ նրանք պատրաստել էին Քաղաքացիական հասարակության հռչակագիրը, մի փաստաթուղթ, որը Ժնևում WSIS-ի հանդիպման ժամանակ ընդունված հիմնական հռչակագրի այլընտրանքն է:

ՀԿ-ներ և WSIS

Ոչ կառավարական հիմնական կազմակերպությունների մասնակցությունը (ՄԱԿ-ի տնտեսական ու սոցիալական խորհրդին կից գրանցված՝ ՄԱԿ-ի ՏՍԽ) WSIS-ի աշխատանքներին խիստ սահմանափակ էր: ՄԱԿ-ի ՏՍԽ-ին կից խորհրդակցական կարգավիճակ ունեցող ոչ կառավարական 3000 կազմակերպությունների փոստից միայն 300-ն է մասնակցել WSIS-ին:

WGIG-ում քաղաքացիական հասարակությունն աշխատանքային խմբի բազմակողմանի բնույթի շնորհիվ ավելի լայնորեն էր ներկայացված: Քաղաքացիական հասարակության կազմակերպությունները WGIG-ին մասնակցելու համար առաջարկել էին ութ թեկնածու, որոնց հավանություն էր տվել ՄԱԿ-ի գլխավոր քարտուղարը: WSIS-ի թունիսյան փուլի ժամանակ քաղաքացիական հասարակության հիմնական ջանքերն ուղղվեցին դեպի WGIG, որտեղ նրանք կարողացան ազդեցություն գործել ընդունված շատ որոշումների վրա, այդ թվում՝ համացանցի օգտագործմամբ կառավարման ֆորում (IGF) ստեղծելու որոշման վրա՝ որպես տարածություն տարբեր շահագրգիռ կողմերի մասնակցությամբ համացանցի կառավարման հարցերի քննարկման համար:

Միջազգային կազմակերպություններ

WSIS գործընթացում միջազգային հիմնական կազմակերպությունը ՀՄՄ-ն էր, որը կազմակերպել էր WSIS-ի քարտուղարության աշխատանքը և մասնակցել կարևորագույն հարցերի վերաբերյալ քաղաքականության մշակմանը: ՀՄՄ-ի մասնակցությունը WSIS գործընթացին կապված է համացանցից ավելի ու ավելի մեծ կախվածություն ունեցող համաշխարհային հեռահաղորդակցության արագ փոփոխվող ասպարեզում իր դիրքերը որոշելու և ամրապնդելու այդ կազմակերպության ակտիվ փորձերի հետ: Համաշխարհային հեռահաղորդակցության ոլորտում ՀՄՄ ազդեցությանը սպառնում են այնպիսի միտումներն, ինչպիսիք են, օրինակ՝ հեռահաղորդակցության համաշխարհային շուկայի ազատականացումը, որն անցկացվում է ԱՀԿ շրջանակներում, և հեռահաղորդակցությունների ավանդական ալիքներից հեռախոսային թրաֆիկի փոխանցումը համացանցին (Voice over IP տեխնոլոգիայի օգնությամբ): Այն, որ WSIS-ի տվյալների համաձայն, ՀՄՄ-ն կարող է դե ֆակտո դառնալ «Համացանցի միջազգային կազմակերպություն», ԱՄՆ-ում և մի շարք զարգացած երկրներում մտահոգություն առաջացրեց, թեև որոշ զարգացող պետությունների աջակցությունն ստացավ: WSIS-ի ամբողջ գործընթացում այդ հեռանկարն ստեղծեց թաքուն լարվածություն: Դա հատկապես նկատելի էր համացանցի կառավարման ոլորտում, որտեղ ICANN-ի և ՀՄՄ-ի միջև լարվածությունը գոյություն ուներ 1998 թ. ICANN-ի ստեղծման պահից ի վեր: WSIS-ը չթուլացրեց այդ լարվածությունը: Հաշվի առնելով հեռահաղորդակցությունների տարբեր տեխնոլոգիաների աճող ինտեգրումը, միանգամայն հավանական է, որ համացանցի կառավարման ընագավառում ՀՄՄ-ի ավելի նշանակալի դարձող դերի մասին հարցը կրկին կհայտնվի քաղաքական քննարկումներում: Հարցերից մեկն էլ վերաբերում էր ՄԱԿ-ի մասնագիտացված գործակալությունների կառուցվածքում WSIS-ի կարգապահական օրակարգի «վայրէջքին»: Հեռահաղորդակցությունների և համացանցային տեխնոլոգիաների ոչ տեխնիկական կողմերը (սոցիալական, տնտեսական, մշակութային հարցերը) մտնում են ՄԱԿ-ի այլ կազմակերպությունների մանդատի մեջ: Այս համատեքստում առավել նկատելի դեր է խաղում ՅՈՒՆԵՍԿՕՆ, որն զբաղվում է այնպիսի հարցերով, ինչպիսիք են՝ բազմալեզվությունը, մշակութային բազմազանությունը, գիտելիքների հասարակությունը ու տեղեկատվության փոխանակումը: WSIS գործընթացում մեծ ջանքեր են ուղղվել ՀՄՄ-ի և ՄԱԿ-ի համակարգի մյուս կազմակերպությունների միջև հավասարակշռության պահպանմանը: Դա պահպանվում է նաև WSIS-ի նախաձեռնած գործընթացներում, որոնց հիմնական մասնակիցներն են ՀՄՄ-ն, ՅՈՒՆԵՍԿՕՆ և ՄԱԿ-ի զարգացման ծրագիրը (ՄԱԿԶԾ):

Այլ մասնակիցներ

WSIS-ի շրջանակներում պաշտոնապես ընդունված շահագրգիռ կողմերից բացի, այլ դերակատարները՝ համացանցային միությունները և ICANN-ը, գործընթացին մասնակցել են քաղաքացիական հասարակության և գործարար հատվածի մեխանիզմների միջոցով:

Համացանցային միություն

Համացանցային միությունը բաղկացած է ինստիտուտներից ու անհատներից, որոնք զարգացնում և խթանում են համացանցն ստեղծման պահից: Պատմականորեն համացանցային միությունների անդամները կապված էին ԱՄՆ բուհերի հետ, որտեղ նրանք մշակում էին տեխնիկական ստանդարտները և համացանցի հիմնական գործառույթը: Այդ միության շրջանակներում ստեղծվել է նաև «համացանցի ավանդական ոգին», որը հիմված էր ռեսուրսների փոխանակման, ազատ հասանելիության և համաշխարհային ցանցի կարգավորման գործում կառավարության մասնակցությանը հակազդելու սկզբունքների վրա: Միության անդամները միշտ պաշտպանում էին համացանցի վաղեմի հայեցակարգը ավելորդ առևտրայնացումից և կառավարության չափից ավելի մեծ ազդեցությունից: Միջազգային հարաբերությունների համատեքստում համացանցային միություններն իրենցից ներկայացնում են էպիսթեմիկ միություն[11]: Սկզբնական փուլում համացանցային միությունը կարգավորվում էր մի քանի, հիմնականում ոչ պաշտոնականացված կանոններով և մեկ պաշտոնական ընթացակարգով՝ մեկնաբանությունների հրցումով (Request for Comments, RFC): Համացանցի հիմնական ստանդարտները նկարագրված են RFC-ի օգնությամբ: Չնայած խիստ կանոնների և պաշտոնական կառուցվածքի բացակայությանը, վաղ փուլերում համացանցային միությունները կարգավորվում էին ըստ ավանդության և մասնակիցների միմյանց վրա թողած ազդեցությամբ: Գործընթացի մասնակիցների մեծամասնությունը կիսում էր ընդհանուր արժեքները, առաջնահերթությունները և առանցքային հարցերի հանդեպ վերաբերմունքը: 1990-ականների կեսերին, երբ համացանցը դարձել էր համաշխարհային հասարակական և տնտեսական կյանքի մի մասնիկը, կասկածի էր ենթարկված համացանցային միությունների ուժերով համաշխարհային ցանցի տեխնիկական կարգավորումը: Համացանցի աճը հանգեցրեց նոր շահագրգիռ կողմերի ի հայտ գալուն (օրինակ՝ բիզնեսի),

Տերմինաբանություն

«Համացանցային միություն» տերմինի հետ միասին այդ նույն հասկացությունը նշելու համար կիրառվում են «համացանցի երևակողներ»,«համացանցիհիմնադիրներ», «համացանցի հայրեր» և «տեխնոլոգներ» բառակապակցությունները: Մենք կիրառում ենք «համացանցային միություն» տերմինը, քանի որ այն ենթադրում է որոշակի արժեքների առնչությամբ անդամների միջև ավելի հստակ համաձայնություն: Բոլորի համար ընդունելի այդ արժեքները միության հատկանշական գծերից մեկն է:

որոնք ներմուծեցին այլ մասնագիտական մշակույթ և ըմբռնումն այն բանի, թե ինչ է համացանցը և ինչպես պետք է այն կառավարել: Դա էլ հանգեցրեց լարվածության աճի: Այսպես, 1990-ականներին համացանցային միությունն ու Network Solutions ընկերությունն ընդգրկված էին, այսպես կոչված, DNS պատերազմում, որը բախում էր առանցքային սպասարկուներին և դոմենային անունները վերահսկելու համար: Ներկայում համացանցային միությունը ներկայացնում են համացանցի հասարակությունը (Internet Society, ISOC) և համացանցի նախագծման աշխատանքային խումբը (Internet Engineering Task Force, IETF):

DNS պատերազմի մասին մանրամասն բաժին 1-ում

ISOC-ը կարևոր դեր է խաղացել համացանցի ստանդարտների մշակման և ներդրման ու այնպիսի հիմնական արժեքների խթանման գործում, ինչպիսին է բաց լինելը: Այն նաև ակտիվորեն մասնակցում է ներուժի զարգացմանը և օգնում է զարգացող, առավելապես աֆրիկյան երկրներին ստեղծելու բազային համացանցային ենթակառուցվածք: Համացանցային միությունը ICANN-ի ստեղծման և գործառնության ընթացքի կարևոր մասնակիցներից մեկն էր: Համացանցը ստեղծողներից մեկը՝ Վինտ Սերֆը այդ կազմակերպության տնօրենների խորհրդի նախագահն էր: Համացանցային միության անդամները կարևոր պաշտոններ են գրավում ICANN-ի տարբեր կառույցներում: Սակայն ներկայում համացանցային միությանն ուղղված քաղաքականության մշակման մոդելը կասկածի է ենթարկվում: Քննադատները նշում են, թե այնքանով, որքանով վերանում է քաղաքացիների և համացանցի օգտատերերի միջև սահմանը, համաշխարհային ցանցի կառավարման գործում ավելի շատ է պահանջվում կառավարության և այլ կառույցների մասնակցությունը, որոնք ներկայացնում են քաղաքացիների, այլ ոչ թե միայն օգտատերերի կազմակերպությունները՝ «համացանցային միությունները»: Այս փաստարկը հատկապես հաճախ են օգտագործում նրանք, ովքեր հնդես են գալիս համացանցի կառավարման գործում կառավարությունների դերի ընդլայնման օգտին:

Համացանցային միությունը սովորաբար համացանցի կառավարման գործում իր առանձնահատուկ դիրքորոշումը հիմնավորում է տեխնիկական հատուկ գիտելիքներով: Նրա ներկայացուցիչներն ընդգծում են, որ ICANN-ը նախևառաջ տեխնիկական կազմակերպություն է, այդ պատճառով էլ այն պետք է ղեկավարեն տեխնիկական գիտելիքների վրա հիմնվող մասնագետները: Քանի որ ICANN-ի գործունեությունը միայն տեխնիկական հարցերով սահմանափակելը ավելի դժվարանում է, ապա այդ հիմնավորումը հաճախ ենթարկվում է քննադատության: Միանգամայն հավանական է, որ համացանցային միության անդամներն աստիճանաբար ընդգրկվում են մասնակիցների այլ, առավելապես քաղաքացիական հասարակության և բիզնեսի, սակայն նաև կառավարության առանցքային խմբերում: Համացանցային միությունը թեև կարող է վերանալ որպես առանձին շահագրգիռ կողմ, սակայն կարևոր է պահպանել այն արժեքները, որոնք նա առաջ է քաշում՝ բաց լինել, գիտելիքների փոխանակում և համացանցի օգտատերերի շահերի պաշտպանություն:

Համացանցում անունների և համարների շնորհման կորպորացիա (ICANN)

Համացանցում անունների և համարների շնորհման կորպորացիան (ICANN) համացանցի կառավարման հիմնական կառույցն է: Դրա պատասխանատվության ոլորտում ընդգրկվում է դոմենային անունների համակարգի կառավարումը (DNS)՝ համացանցի հիմնական ենթակառուցվածքը, որը կազմված է IP հասցեներից, դոմենային անուններից և արմատական սպասարկուներից: ICANN-ի հանդեպ հետաքրքրությունն աճել է 2000-ականներին համացանցի արագ աճի հետ միասին, և WSIS-ի ընթացքում ICANN-ը գտնվում էր համաշխարհային քաղաքական շրջանակների ուշադրության կենտրոնում: ICANN-ը թեև համացանցի կառավարման գործընթացի գլխավոր մասնակիցն է, սակայն այն չի կարգավորում համացանցի բոլոր կողմերը, այդ պատճառով ճիշտ չէ այն անվանել «համացանցի կառավարություն», ինչը հաճախ են անում: ICANN-ը կառավարում է համացանցային ենթակառուցվածքը, սակայն լիազորություններ չունի համացանցի կառավարման մյուս կողմերի նկատմամբ, ինչպիսիք են՝ կիբեռանվտանգությունը, բովանդակության (կոնտենտի) վերահսկողությունը, հեղինակային իրավունքների պաշտպանությունը, գաղտնիության պահպանումը, մշակութային բազմազանության պահպանումը կամ թվային բաժանման հաղթահարումը: ICANN-ը Կալիֆորնիայում գրանցված ոչ առևտրային միավորում է: Դրա գործառնական լիազորությունները հիմնված են ԱՄՆ առևտրի նախարարության և ICANN-ի միջև փոխըմբռնման մասին հուշագրի վրա, որը ստորագրվել է 1998 թ. և երկու անգամ երկարացվել (երկրորդ անգամ՝ 2006 թ. սեպտեմբերից մինչև 2009 թ. սեպտեմբերը): 2009 թ. հոկտեմբերի 1-ի դրությամբ ICANN-ի գործառնության պաշտոնական հիմքը «Պարտականությունների հաստատումն» է (Affi rmation of Commitments): ICANN-ի և ԱՄՆ առևտրի նախարարության միջև ստորագրված այդ փաստաթուղթը ծառայում է որպես հիմք ICANN-ը անկախ կազմակերպություն դարձնելու համար:

ICANN-ը բազմակողմ կազմակերպություն է, որն ընդգրկում է տարբեր լիազորություններով ու դերերով մասնակիցների լայն շրջան: Նրանք բաժանվում են չորս հիմնական խմբի: Առաջին խումբը կազմված է նրանցից, ովքեր ICANN-ի գործունեությանը մասնակցել են ստեղծման պահից՝ համացանցային միությունները, գործարար միությունները և ԱՄՆ կառավարությունը:

Երկրորդ խումբն ընդգրկում է միջկառավարական կազմակերպություններ, որոնց շարքում կարևոր դեր են կատարում Հեռահաղորդակցության միջազգային միությունը և Մտավոր սեփականության համաշխարհային կազմակերպությունը:

Երրորդ խումբը կազմված է ազգային կառավարություններից, որոնք 2003թ. WSIS-ից սկսած ցանկանում են առավել նշանակալի դեր խաղալ ICANN-ում:

Չորրորդ խումբը ներառում է համացանցի օգտատերերին («բոլորի միություն»): ICANN-ը փորձեր է կատարել տարբեր մոտեցումները, փորձելով կառավարման համակարգում ներգրավել համացանցի օգտատերերին: Նրա գոյության սկզբնական փուլերում փորձեր են արվել անմիջական ընտրություններով ղեկավար մարմիններում օգտատերերի ներկայացուցիչներին ընտրել, ինչը կոչված էր ICANN-ի իրավական բազան ամրապնդելու: Ընտրողների թույլ ակտիվության և խախտումների պատճառով անմիջական ընտրությունները չկարողացան ապահովել օգտատերերի իրական ներկայացուցչություն:
Վերջին ժամանակներում ICANN-ը փորձում է իր գործունեության մեջ ներգրավել համացանցի օգտատերերին՝ կառավարման «բոլորին ներկայացնող» (atlarge) կառույցի միջոցով: Կազմակերպչական այդ փորձը դեռևս շարունակվում է:
ICANN-ում որոշումներ ընդունելու գործընթացի վրա ազդեցություն են գործել համացանցի կառավարման վաղ շրջանի մոդելները, որ հիմնված էին ժողովրդավարության, թափանցիկության, բաց լինելու և համընդհանուրի մասնակցության սկզբունքների վրա: ICANN-ում որոշումներ ընդունելու հարցում 1980-ականների համացանցային միությունների և ներկա համատեքստի միջև հիմնական տարբերությունը «սոցիալական կապիտալի» մակարդակն է: Նախկինում համացանցային միությունը փոխադարձ վստահության և համերաշխության ավելի էր արժանանում, ինչը նշանակալիորեն հեշտացնում էր որոշումներ ընդունելու և վեճերը լուծելու գործընթացը: Համացանցի տարածումը հանգեցրեց շահագրգիռ կողմերի բազմազանության և քանակի ավելացման, համապատասխանաբար, այդ մասնակիցների սոցիալական կապիտալի մակարդակը շատ ցածր է: Այդ պատճառով համացանցի զարգացման սկզբնական փուլերում գոյություն ունեցող որոշումներ ընդունելու ընթացակարգը պահպանելու մասին համացանցային միության պահանջը, հիմնականում, ուտոպիական է: Առանց սոցիալական կապիտալից կախվածության, որոշումներ ընդունելու գործընթացի գործառնությունն ապահովելու միակ միջոցը զսպելու և հակակշռելու տարբեր մեխանիզմների մշակումն ու պաշտոնականացումն է: Որոշումներ ընդունելու ընթացակարգի որոշ փոփոխություններ, որոնք նոր իրողություններ են արտացոլում, արդեն կատարված են: Դրանցից ամենակարևորը 2002 թ. ICANN-ի բարեփոխումն էր, որի մի մասն էր կազմում կառավարության խորհրդակցական կոմիտեի ուժեղացումը և անմիջական քվեարկության համակարգից հրաժարվելը:

Հարցեր

Տեխնիկական կամ քաղաքական հարցերի լուծում

Տեխնիկական և քաղաքական հարցերի լուծման միջև հակասությունները միշտ էլ լարվածություն է ստեղծել ICANN գործունեության ընթացքում: ICANN-ն ընկալվում է որպես «տեխնիկական համակարգող կառույց», որը

զբաղվում է միայն տեխնիկական հարցերով և չի շոշափում համացանցի քաղաքական տեսանկյունները: ICANN-ի պաշտոնատար անձինք այդ առանձնահատուկ տեխնիկական բնույթը համարում էին հիմնական հայեցակարգային փաստարկն ի պաշտպանություն կազմակերպության եզակի կարգավիճակի և կազմակերպչական կառուցվածքի: ICANN-ի առաջին նախագահ Եսթեր Դայսոնն ընդգծել է, որ ICANN-ը չի ձգտում համացանցի կառավարման բոլոր հարցերը լուծել, ըստ էության այն կառավարում է ենթակառուցվածքը, այլ ոչ մարդկանց: Նրա մանդատը սահմանափակված է, ընդհանուր առմամբ, համացանցի ենթակառուցվածքի որոշակի (առավելապես տեխնիկական) կողմերի վարչարարությամբ և, մասնավորապես, DNS-ով[12]: Այս պնդման քննադատները սովորաբար մատնանշում են, որ տեխնիկապես չեզոք լուծումներ գոյություն չունեն: Վերջին հաշվով, յուրաքանչյուր տեխնիկական որոշում առաջ է քաշում որոշակի շահեր, ամրապնդում է որոշակի խմբերի և ազդում է հասարակական, քաղաքական ու տնտեսական կյանքի վրա: «xxx» դոմենի ստեղծման («մեծ» նյութերի համար) հնարավորության վերաբերյալ բանավեճերը բացահայտ ցույց են տալիս, որ ICANN-ը ստիպված զբաղվելու է տեխնիկական հարցերի քաղաքական տեսակետներով:

ICANN-ի միջազգային կարգավիճակը

ICANN-ի և ԱՄՆ կառավարության միջև հատուկ կապերը միշտ երկու ուղղությամբ տարվող քննադատության են ենթարկվել: Առաջինը սկզբունքային նկատառումներով է արվում և շեշտը դնում է այն բանի վրա, որ բոլորի համար կարևոր համացանցի համաշխարհային ենթակառուցվածքի կարևորագույն տարրը գտնվում է մեկ պետության վերահսկողության ներքո: Այս քննադատությունն ակնհայտ էր WSIS-ի ընթացքում և ուժեղանում էր Իրաք ռազմական ներխուժումից հետո ԱՄՆ-ի արտաքին քաղաքականության հանդեպ համընդհանուր թերահավատության պատճառով: Քննարկումների այս մակարդակում քննադատությանն ի պատասխան հաճախ առաջ էր բերվում այն փաստը, որ համացանցը ստեղծվել է ԱՄՆ կառավարության ֆինանսական աջակցությամբ: Դա ԱՄՆ կառավարությանը բարոյական հիմք է տալիս որոշումներ կայացնելու համացանցի կառավարման ինտերնացիոնալացման ձևի և տեմպերի վերաբերյալ: Այդ փաստարկը մեծ աջակցության արժանացավ հատկապես ԱՄՆ Կոնգրեսում, որը միանշանակ դեմ է համացանցի կառավարման ցանկացած ինտերնացիոնալացմանը: ICANN-ի ինտերնացիոնալացման օգտին փաստարկների երկրորդ ուղղությունը հիմնված է գործնական և իրավաբանական նկատառումների վրա: Այսպես, որոշ քննադատներ այն կարծիքն էին հայտնում, որ եթե ԱՄՆ-ի դատական իշխանությունները օգտագործեն իրենց լիազորությունները և պատժամիջոցներ կիրառեն Իրանի ու Կուբայի նկատմամբ, ապա կարող են ICANN-ին պարտադրել, որ այն՝ որպես ամերիկյան մասնավոր ընկերություն, համացանցից ջնջի այդ երկու պետությունների ազգային

դոմենները: Այս փաստարկի համաձայն, շարունակելով պահպանել Իրանի և Կուբայի դոմենային անունները, ICANN-ը խախտում է պատժամիջոցների վերաբերյալ ԱՄՆ օրենքը: Թեև ազգային դոմենների վերացման նախադեպ դեռևս չի եղել, սակայն ICANN-ի գոյություն ունեցող իրավական կարգավիճակում այդպիսի իրավիճակի հավանականությունը պահպանվում է: ICANN-ի կարգավիճակի մասին քննարկումների նոր փուլ սկսելու ազդանշան է համարվում ԱՄՆ առևտրի նախարարության և ICANN-ի միջև «Պարտականությունների հաստատման մասին» փաստաթղթի ստորագրումը: Այդ իրադարձությունը ICANN-ի անկախության հիմքն է դնում և առաջ է քաշում հարցերի մի նոր շարք, որոնք վերաբերում են այդ կազմակերպության վերահսկողությանը, պատասխանատվությանը, կառավարությունների հետ հարաբերություններին և այլն: Երկու հիմնական հարց՝քաղաքական տեսանկյունների նկատմամբ լիազորությունները և միջազգայնացումը, կարող են լուծվել ICANN-ի կարգավիճակի փոփոխմամբ, ինչը թույլ կտա նվազեցնել կարգավիճակի անորոշությունը և բարձրացնել կազմակերպության առաքելության թափանցիկությունը: ICANN-ի զարգացումը հետագայում կպահանջի նոր լուծումներ: Հավանական փոխզիջում կարող է լինել ICANN-ի փոխակերպումը միջազգային հատուկ կազմակերպության, որը կպահպանի ICANN-ի գոյություն ունեցող կառուցվածքի առավելությունները, միաժամանակ հաղթահարելով թերությունները, հատկապես միջազգային լեգիտիմության հիմնախնդիրը:

Ծանոթագրություններ

1. Բացառություն են ԱՄՆ-ն և մի շարք զարգացած երկրներ (Ավստրալիան, Նոր Զելանդիան և դրանց շարքում՝ Եվրախորհուրդը)

2. WGIG անդամների ընտրությունը հիմնված էր ներկայացուցչական չափանիշների և փորձագիտական հմտությունների վրա: Ներկայացուցչական կառուցվածքը հիմնված էր կառավարությունների, քաղաքացիական հասարակության և բիզնեսի շրջանակներից մասնակիցների հավասար քանակի ապահովման սկզբունքի վրա (ընդհանուր թվի 1/3-ը): Կառավարությունների ներկայացուցիչներն ընտրվում էին ՄԱԿ-ի տարածաշրջանային խմբերի համար սովորական չափանիշներով: Ներկայացուցչականության նկատառումների հետ մեկտեղ պահանջվում էր, որպեսզի ընտրված մասնակիցները բավականաչափ գիտելիքներ ունենային WGIG-ի քննարկման առարկայի մասին, որպեսզի դրանցում իմաստալից ներդրում կատարեին:

3. Տես՝ «Տեղեկատվական հասարակության հարցերի վերաբերյալ համաշխարհային բարձր մակարդակի հանդիպում»: «Սկզբունքների հռչակագիր»: WSIS-03/GENEVA/DOC/4-R, 12 դեկտեմբերի, 2003 թ., էջ՝ 49:

4. Ազգային դոմենի կառավարման բրազիլական մոդելը սովորաբար բերվում է որպես բազմակողմանի մոտեցման հաջողված օրինակ: Բրազիլիայի ազգային դոմենի համար պատասխանատու կազմակերպությունը բաց է բոլոր օգտատերերի համար, ներառյալ կառավարական գերատեսչությունները, գործարար հատվածը և քաղաքացիական հասարակությունը: Բրազիլիան այդ մոդելն աստիճանաբար տարածել է նաև համացանցի կառավարման մյուս ոլորտներում, հատկապես Ռիո դե Ժանեյրոյում տեղի ունեցած IGF-2007 նախապատրաստական գործընթացում:

5. Charles Lesage, La rivalite franco-britannique. Les cables sous-marins allemands (Paris, 1915) p. 257-258; цит. по: Daniel R. Headrick, Th e Invisible Weapon: Telecommunications and International Politics 1851-1945 (Oxford University Press: 1991), p. 110.

6. Cukier, K. N. (2005). Th e WSIS wars: an analysis of the politicization of the Internet.

In: B: D. Stauff acher and W. Kleinwachter (eds). Th e World Summit on the Information

Society: moving from the past into the future. New York: United Nations ICT

Task Force, p. 176.

7. ԱՄՆ կառավարությունը իր ուղարկած հեռագրում քննադատել էր ՀՄՄ-ի մասնակցությունը CORE նախագծին, որում ասվում էր. «Առանց անդամ պետությունների կառավարությունների հաստատման հրավիրվել է համաշխարհային հանդիպում, որը ենթադրելի է, որ չի հաստատել ռեսուրսների ծախսերը և «միջազգային համաձայնագրերի» եզրակացությունը»:

8. «Մեկ պատուհանի» հարմարավետությունը այն փաստարկներից մեկն էր, որ ՀՄՄ-ին հաստատում էր որպես համացանցի կառավարման գործում որպես գլխավոր դեր խաղացող:

9. Այդ հարցի վերաբերյալ արժեքավոր գնահատականներ է տվել Աիշա Հասանը (Ayesha Hassan)

10. Վեճերի լուծման միասնական քաղաքականության մշակում (Universal Dispute Resolution Procedures – UDRP)

11. Համացանցային միությունը համապատասխանում է Փիթեր Հասի առաջադրած էպիստեմիկ միության չափանիշներին. «Արհեստավարժ խումբ, որի անդամները ընդհանուր պատկերացում ունեն իսկության ստուգման մեթոդների, պատճառների և հետևանքների մասին, կիսում են ընդհանուր արժեքները, ունեն հիմնախնդիրների և դրանց լուծման մասին ընդհանուրը մբռնում» (Peter Haas (1990), Saving the Mediterranean: the politics of international environmental co-operation (New York: Columbia University Press, p. 55)

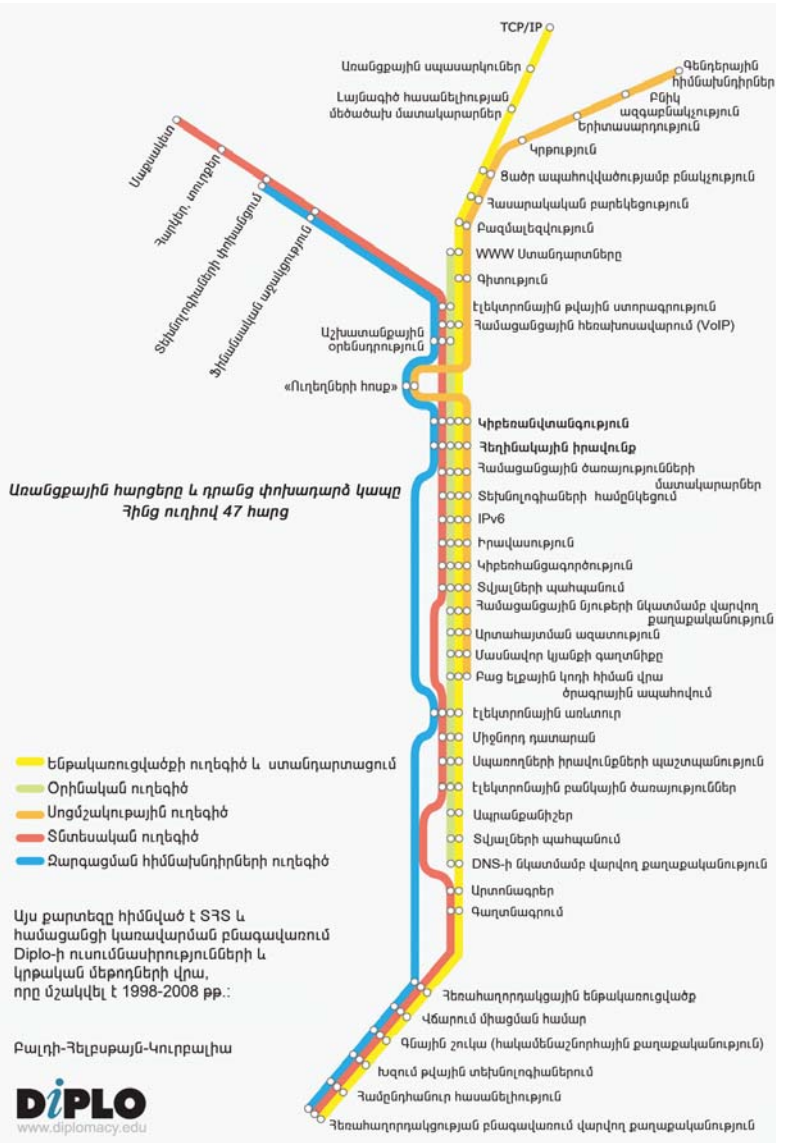
12. Տես՝ Esther Dyson's Response to Ralph Nader's Questions. 15 June 1999 (համացանցային հասցեն՝ http://www.icann.org/correspondence/dyson-response-to-nader-15jun99.htm):

Բաժին 8

Հավելված

Հավելված 1

Ճանապարհորդություն համացանցի կառավարման երթուղով



Հավելված 2

Համացանցի օգտագործմամբ կառավարման վերաբերյալ ֆորումի տասնչորս դասերը

Համացանցի օգտագործմամբ կառավարման վերաբերյալ ֆորումի (IGF) ընթացքում ներկայացվել է համաշխարհային քաղաքական գործընթացների կառավարման մի քանի նորարարական մոտեցումներ: Դրանցից մի քանիսը կարող են օգտակար լինել նաև քաղաքականության այլ բնագավառների համար, շոշափելով շահագրգիռ շատ կողմերի շահերը (օրինակ՝ կլիմայի փոփոխությունը, միգրացիան, առևտուրը, մարդու իրավունքները): IGF փորձը քննարկելիս շատ կարևոր է նկատի ունենալ համացանցի կառավարման և համաշխարհային քաղաքական այլ գործընթացների միջև մեկ էական տարբերություն: Այն դեպքում, երբ կարգավորման այլ բնագավառները, ինչպիսին է կլիմայի փոփոխությունը, ավանդաբար վերահսկում էին պետություններն ու դանդաղորեն բացվում էին ոչ պետական ատյաններում դեր խաղացողների համար, համացանցի կառավարման բնագավառում կառավարությունները ստիպված էին ներգրավվել արդեն գոյություն ունեցող ոչ պետական կառավարական կարգում, որի կենտրոնը ICANN-ն է: IGF-ն այդ գործընթացում կարևոր տարրերից մեկն է: Նրա համապատասխան փորձը կարելի է ամփոփել հետևյալ տասնչորս հանձնարարականներում.

1.Դարձեք ազդու առաջնորդ. «Իմաստուն՝ բեմի վրա և ուղեկցող՝ ճանապարհին»

IGF-ի հաջողության հիմնական պատճառներից մեկը այն նախագահող Նիթինա Դեսայիի և IGF-ի քարտուղարության գործադիր համակարգող Մարկուս Կումերի ղեկավարման բացառիկ մակարդակն է: Ն. Դեսային և Մ. Կումերը միասին կազմում են ազդեցիկ թիմ՝ լրացնելով միմյանց հայացքներն ու հմտությունները: Երկուսն էլ ունեն դիվանագիտական մեծ փորձ. Դեսային պատասխանատու էր ՄԱԿ-ում բարձր մակարդակի մի շարք հանդիպումների նախապատրաստման համար, իսկ Կումերը հաջող կարիերա ունի Շվեյցարիայի դիվանագիտական կարույցներում: Քանի դեռ Դեսային ղեկավարում էր IGF-ի միջոցառումների «գլխավոր

բեմը», Կումերը մասնակիցներին օգնում էր հասնելու փոխըմբռնման և ընդգրկվել գործընթացի մեջ, անհրաժեշտ պահին նրանց հետ համացանցի միջոցով շփվելով պաշտոնական հանդիպումների շրջանակներից դուրս, և մասնակցելով IGF-ի շուրջ հավաքված տարբեր մասնագիտական միությունների հիմնական միջոցառումներին:
ՄԱԿ-ի կանոնների, ընթացակարգերի և պրակտիկայի խորը գիտելիքներն այդ երկու դիվանագետներին օգնեցին գտնելու ստեղծագործական լուծումներ և ստեղծելու արդյունավետ, թեև ոչ պաշտոնական ֆորումի modus operandi 1: Դեսային IGF-ի հիմնական հաջողություններից մեկը բացատրում է հետևյալ կերպ. «Որպեսզի երկխոսությունը կայանա, բոլոր մասնակիցները պետք է ընդունեն, որ տվյալ ֆորումի արժեքը մյուս մասնակիցների ներկայությունից է կախված, սակայն արդյունավետ երկխոսության համար յուրաքանչյուր մասնակից իր սպասումները մյուսների նկատմամբ պետք է կարգավորի և, առաջին հերթին, պետք է լսի, ոչ թե խոսի»:
Համացանցի կառավարման բնագավառում նորեկներ Ն. Դեսային և Մ. Կումերը ICANN-ի վերաբերյալ երկար քննարկումներում (դոմենային անուններ, IP հասցեներ և առանցքային սպասարկուներ) որևէ «կուսակցության» չեն պատկանում: Նրանց հաջողությունը կասկածի ենթարկեց «դիվանագիտական այն առասպելը», ըստ որի տեխնիկական հարցերը պետք է լուծեն տեխնիկայի փորձագետները: Ինչպես ցույց է տալիս այս օրինակը, երբեմն տեխնիկական հարցերի լուծման «դիվանագիտացումը» կարող է օգնել հաղթահարելու ավանդական վեճերը՝տեխնիկայի մասնագետների միություններում և նպաստել քաղաքական գործընթացի հաջողությանը:
1. Գործունեության ձևը, գործելու ձևն է (լատ.), Նիթին Դեսայի և Մարկուս Կումեր

2. Կառուցեք վստահելի հարաբերություններ՝ գործելով ժամանակին և ճիշտ հերթականությամբ

IGF գործընթացը մեկ սեղանի շուրջ հավաքեց տարբեր մասնագիտությունների եւ մշակույթների տեր և փորձ ունեցող մարդկանց: Մասնակիցները միևնույն կազմակերպություններում չէին ձեռք բերել իրենց փորձը, միևնույն համալսարաններում չէին սովորել, չէին աճել նույն սոցիալական շրջանակներում և այլ հիմնական բաղադրիչներում, որի վրա հիմնված ստեղծվում է վստահությունը: Վստահության փոխհարաբերությունները ստեղծվեցին միանգամայն կասկածամտության մթնոլորտում, որն ստեղծվել էր կամ նախկին վեճերի պատճառով (օրինակ՝ ՀՄՄ-ի և ICANN-ի միջև), կամ Իրաքի պատերազմից առաջացած համընդհանուր աշխարհաքաղաքական լարվածությունից, կամ պարզ մարդկային «մեզ» և «նրանց» հակադրության հետևանքով:
Վստահության փոխհարաբերություններ ստեղծելը պահանջում է համբերություն և գործողությունների ճիշտ ծրագրված հետևողականություն:

IGF գործընթացի յուրաքանչյուր փուլն ուղղված է փոխըմբռնման նվաճումների և նոր գիտելիքներ ու տեղեկատվություն ձեռքբերմանը: Դրա արդյունքը եղավ այն, որ աստիճանաբար ամրապնդվեց վստահությունը, իսկ քննարկումները դարձան բովանդակալից: Որոշ առաջարկություններ, ինչպիսին էր, օրինակ՝ բանակցությունների սկզբում հնչած կոչը՝ համացանցի մասին շրջանակային պայմանագիր ընդունելու վերաբերյալ, արդարացիորեն մերժվեցին. համացանցի կառավարման հետագա պաշտոնականացման համար ժամանակը դեռևս չի հասունացել: ICANN-ի ապագայի մասին ԱՄՆ կառավարության վերջերս ընդունած որոշումը ցույց տվեց, որ որոշ հիմնախնդիրներ ժամանակի ընթացքում կորցնում են իրենց հրատապությունը, եթե դրանց հետ զգուշորեն են վարվում և թույլ չեն տալիս վերածվել քաղաքական ճգնաժամի: IGF-ն այդ առումով միանգամայն հաջողված էր:

Դիվանագետներն ու քաղաքագետները կարող են IGF-ից սովորել վստահության արդյունավետ փոխհարաբերությունների ստեղծում՝ ճիշտ պահին ընտրելու և հետևողական գործողությունների շնորհիվ, նուննն է թե նոր բան հասկանալ, ընդհանուր առմամբ, քաղաքական գործընթացում ժամանակի և ժամկետների մասին:

3.Թույլ տվեք քաղաքական գործընթացը իր հունով զարգանա

Պահի ճիշտ ընտրության հետ սերտորեն կապված է մեկ այլ երաշխիք՝ շատ կարևոր է թույլ տալ, որ գործընթացները զարգանան սեփական իներցիայով և հույս չդնել շատ մանրակրկիտ ծրագրման վրա: Արդի աշխարհում տրամաբանորեն հաջորդական նախագծերի մշակումն ու «մուտք- ելք» մեթոդով վերահսկողությունը նման է սևեռուն գաղափարի: Գործընթացների այսպիսի մանրակրկիտ կառավարումը կարող է անարդյունավետ լինել, քանի որ սոցիալական իրականությունը բավականին բարդ է, որպեսզի այն դրվի մոդելների ու նախագծերի «պրոկրուստյան մահիճում»: Վերջին ժամանակների համաշխարհային ֆինանսական ճգնաժամը օրինակ է ծառայում այն բանի, որ հիմնականում գիտության և մոդելավորման վրա հիմնված համակարգը կարող է հասցնել կործանման, եթե հաշվի չեն առնվում մարդիկ իրենց թույլ և ուժեղ կողմերով, իրենց ողջ բարդությամբ: Դիվանագիտության մեջ քաղաքական գործընթացների մանրակրկիտ կառավարման հետ կապված ռիսկերը լավ լուսաբանում են Վիեննայի համաժողովի (1814) հաջողությունը և Վերսալյան պայմանագրի (1919) ձախողումը: Վիեննայի համաժողովը հիմք դրեց Եվրոպայի պատմության ամենախաղաղ ժամանակաշրջաններից մեկի համար, երբ մոտավորապես 100 տարի մեծ պատերազմներ չծագեցին: Վերսալյան խաղաղության պայմանագիրը, հակառակը, ձախողման ենթարկվեց ստորագրվելուց մի քանի տարի հետո: Վիեննայում բանակցությունների մասնակիցները աշխատելու բավականին ժամանակ ունեին, սակայն չէին բացառվել նաև փոխազդեցությունների սոցիալական կողմերը: Աստիճանաբար, առանց նախապես որոշակի ընդհանուր ծրագրի նրանք մշակեցին արդյունավետ

խաղախության համաձայնագիր, ինչը նվաճեցին հանճարեղ Մետեռնիխի ու Թալեյրանի օգնությամբ:
Վերսալում, հակառակը, դիվանագետները մասնակցում էին լավ կազմակերպված գործընթացի, որում հարյուրավոր գիտնականներ, վիճակագիրներ և քարտեզագիրներ միասին աշխատել էին «գիտությամբ կառուցված աշխարհ» ստեղծելու ծրագրի վրա: Նրանք նույնիսկ արդարացի լուծումների որոնումներում փորձում էին կիրառել քանակական մեթոդներ: Արդյունքում այդ ամենը առաջացրեց խառնաշփոթ, որն էլ հանգեցրեց Երկրորդ համաշխարհային պատերազմին:
Այս երկու պայմանագրերի ճակատագրերի վրա շատ այլ գործոններ ևս ազդել են, սակայն բանակցությունների կազմակերպման մոտեցումների էական տարբերությունները համոզիչ վկայությունն են դիվանագիտական գործընթացների չափից ավելի կարգավորման դեմ:

Վիեննայի կոնգրեսի (1814) անկաշկանդ մթնոլորտը
IGF-ը թեև չի կարող համեմատվել այս մեծ իրադարձությունների հետ, այնուամենայնիվ դրա սկզբունքները մոտ են Վիեննայի կոնգրեսին: Շվարճությունները, ցավոք ավելի քիչ էին, քան Վիեննայում, սակայն ընդհանուր էր գործընթացները կանխորոշելու փորձեր չանելու ձգտումը, բացառությամբ նվազագույն պլանավորման: IGF քննարկումները բացվում են և ընդունում լավագույն ձևը՝ մասնակցող կողմերի, այդ թվում նաև էապես տարբեր, կարծիքների «միաձուլման» ճանապարհով:

4. Կիրառեք տարբեր տեսակետներ քաղաքական «երկար պոչի» հաշվին

«Երկար պոչ 2» հայեցակարգը քաղաքականություն մուտք է գործել մարկեթինգից և վերաբերում է տարբեր տեսակետների օգտագործման հնարավորությանը, որոնք սովորական պայմաններում կարող էին կորել միջկառավարական ավանդական փոխազդեցությունների տարբեր զտիչներում: Առանձին մարդիկ և խմբեր կարող էին իրենց կարծիքն արտահայտել անմիջականորեն ֆորումին՝ միջոցառումներին, վեբ հաղորդակցություններին մասնակցելով և հեռավոր մասնակցության ճանապարհով: Այդ նոր գաղափարներն ու կարծիքները, որոնց մեծ մասը չի հասնում բարձր մակարդակի համաժողովներին, նշանակալիորեն հարստացրին IGF-ը: Քաղած դասերից մեկն այն է, որ քաղաքական գործընթացի բացախոսության հասնելու քայլերից մեկը այդ գործընթացներին ազատ մասնակցության հրավիրելն է: Բաց եւ բազմակողմանի մասնակցության առավելության հասնում են այն ժամանակ, երբ հավաքվում, քննարկվում և հնարավորինս քաղաքական փաստաթղթերում ընդգրկվում են առավելագույն մեծ քանակի տեսակետներ: Բանակցությունների գործընթացում տարբեր շահագրգիռ կողմերի ներգրավումը բարձրացնում է այդ բանակցության լեգիտիմությունը և մասնակիցների մոտ արդյունքին մաս կազմելու զգացում է առաջացնում:

5. Ընդլայնեք «դիվանագիտական հետք թողնելու» երկրի հնարավորությունը՝ գրավելով տարբեր շահագրգիռ կողմերի

Ազգային պետությունների և դիվանագիտական ծառայությունների ստեղծման պահից ի վեր 18-րդ դարում երկրի բնակիչների շահերը երկրի սահմաններից դուրս ներկայացնում էին կառավարության ներկայացուցիչները: Ռիշելյեն երբ ստեղծեց Ֆրանսիայի արտաքին գործերի նախարարություն, Փարիզից Մոսկվա նամակները հասնում էին մեկ ամսում: Այսօր այդ տարածությունը հաղորդագրությունները կտրում անցնում են վայրկյանների ընթացքում:

2. Մարկեթինգում «երկար պոչ» արտահայտությունը (առաջին անգամ այն կիրառել է Կրիս Անդերսը Wired ամսագրում տպագրած հոդվածում, որից հետո նաև «Երկար պոչ. բիզնեսի վարման նոր մոդել» գրքում) նշում է այն սպառողներին, ում հետաքրքրում են հատուկ, որմնախորշային, հաճախ քիչ հայտնի ապրանքներ: Դրանց ընդհանուր պահանջարկը կարող է նշանակալիորեն գերազանցել հայտնի ապրանքների ոչ մեծաքանակ վաճառքի ընդհանուր ծավալը, սակայն մինչ էլեկտրոնային առևտրի ի հայտ գալը նյութատեխնիկական ծախսերը շատ մեծ էին, որպեսզի «երկար պոչի» ապրանքների վաճառքը տնտեսապես արդարացված լիներ:

Սա ստիպում է մտածել այն մասին, թե արդյոք դիվանագիտական ներկայացուցչության բնույթը կարող է մնալ նախկինը, չնայած հեռահաղորդակցության բնագավառում տեղի ունեցած արմատական փոփոխություններին: Ներկայացուցչության որոշ տեսակետներ, անշուշտ, անփոփոխ են մնում: Մոտ ապագայում պետությունները կմնան մարդկային հասարակության կազմակերպման հիմնական ձևը, բնութագրվելով որոշակի բնակչության, տարածքի և ընդհանուր ազգային ինքնությամբ: Դիվանագիտությունը պահպանում է իր նշանակությունը՝ որպես երկրի սահմաններից դուրս հասարակության շահերը ներկայացնելու համար գլխավոր խողովակ: Սակայն ներկայացուցչության հայեցակարգը այլ հարաբերություններում պետք է հարմարեցնել: Այն պայմաններում, երբ համաշխարհային ասպարեզում խաղացողներն ավելացան և բարդ հարցերը շատացան, դիվանագիտության ավանդական մոտեցումը լուրջ սահմանափակում է ցուցաբերում: Նույնիսկ ամենաարդյունավետ դիվանագիտական ծառայությունները օտարերկրյա սուբյեկտների հետ շփման համար բավականաչափ չեն տիրապետում «անցագրային ունակությունների» (այսինքն՝հմուտ մարդկային ռեսուրսների):

Առավել բարձր «դիվանագիտության անցագրային ունակություններ» կարելի է ապահովել քաղաքացիական հասարակության, գործարար շրջանակների, իշխանության տեղական մարմինների ներկայացուցիչների և համաշխարհային քաղաքական գործընթացների այլ սուբյեկտների ներգրավելով: Արդեն այսօր շատ ոչ պետական սուբյեկտներ վարում են իրենց սեփական «դիվանագիտությունը», օրինակ՝ կապ են պահպանում օտարերկրյա կազմակերպությունների հետ, մասնակցում են միջազգային խորհրդաժողովների և ձևավորում են համաշխարհային քաղաքական

դասախոսություններ: Որոշ պետություններ, օրինակ՝ Կանադան, Շվեյցարիան և Սկանդինավյան երկրներն առաջինն ընդունեցին այդ միտումը և ոչ պետական մասնակից անձանց ընդգրկեցին արտաքին քաղաքականության գործընթացի մեջ՝ այնպիսի նախաձեռնությունների շնորհիվ, ինչպիսիք են՝ «Կանադայի թիմը» (Team Canada) և ԳԱՄ աշխատանքների գծով հատուկ դեսպանների նշանակումը: Ցավոք, այս պրակտիկան տարածված չէ շատ զարգացող երկրներում, որտեղ «դիվանագիտության անցագրային ունակությունը», որպես կանոն, շատ ցածր է և բավարարվում է սահմանափակ ֆինանսական և մարդկային ռեսուրսներ ունեցող ոչ մեծ դիվանագիտական ծառայությամբ: Շատ զարգացող երկրներում բազմակողմ կառույցներն ազգային մակարդակում ի հայտ են եկել վերջին մի քանի տարվա ընթացքում:

Համացանցի կառավարման վերաբերյալ ֆորումը գործնական ավանդ ներդրեց բազմակողմանի հանդիպումների մոտեցման մասին կառավարության շրջանակների իրազեկվածության բարձրացման գործում, հատկապես զարգացող երկրներում: Բացի մասնակցության բաց լինելու սկզբունքից, IGF-ի շրջանակներում բազմակողմանի մոտեցումը ցույց էր տալիս նաև գործնական լուծում, ինչը օգնում էր երկրներին թողնելու «դիվանագիտական հետք»՝ առանց մեծ ռեսուրսներ ներդնելու անհրաժեշտության:

Ազգային մակարդակում ի հայտ են գալիս IGF-ի բազմակողմանի մարմիններ, և կառավարությունները հաճախ համակարգում են իրենց գործողությունները գործարար շրջանակների և քաղաքացիական հասարակության հետ: Որոշ փոքր և զարգացող պետությունների համացանցի կառավարման գործընթացում ներկայացնում են ոչ պետական սուբյեկտները: Երբեմն այդպիսի բաց մասնակցության ներդրումը համարվում է հիմնականում համակարգման հարց, սեփական երկրի փորձառու ներկայացուցիչների բացահայտում և բազմակողմանի մասնակցության ազգային մեխանիզմի ստեղծում: Օգտակար է նաև ներուժի զարգացման ուղղությամբ ուսումնական ծրագրերի կազմակերպումը տարբեր շահագրգիռ կողմերի մասնակցությամբ, որոնք ներկայացնում են մեկ երկիր. այդպիսի ծրագրերի մասնակիցների միջև, որպես կանոն, հաստատվում են թիմային ոգու և վստահության հարաբերություններ:

6. Բարձրացրեք քաղաքական համաձայնեցվածության մակարդակը՝ գրավելով տարբեր շահագրգիռ կողմերի

Այսօր համաշխարհային քաղաքական ցանկացած գործընթացի համար այդ թվում այնպիսի բնագավառներում, ինչպիսիք են կլիմայի փոփոխությունն ու միգրացիան, հիմնական բարդություններից մեկը միջկարգապահական հարցերի լուծման մեջ քաղաքական համաձայնության հասնելն է: Համացանցի կառավարման ոլորտում IGF-ը հանդես է գալիս որպես «հովանոց», որի ներքո կարող են տեղավորվել գոյություն ունեցող տարբեր կարգեր, ներառյալ տեղեկատվական

տեխնոլոգիաները, մարդու իրավունքները, առևտուրն ու մտավոր սեփականությունը: IGF գործընթացում քաղաքական տարբեր խմբեր բացահայտում են, որ իրենց շահերից բխող նախկինում մեկուսացված ոլորտները համացանցի կառավարման մասն են կազմում: Որոշ թեմատիկ ոլորտներում, ինչպիսին է, օրինակ՝ բազմալեզվությունը, IGF-ը օգնել է տարբեր կազմակերպություններին, ներառյալ կառավարությանը, ICANN, ՅՈւՆԵՍԿՕ-ն և ՀՄՄ-ն, կոորդինացնել ջանքերը՝ ընդհանուր խնդրի լուծման համար: IGF-ը՝ որպես որոշումներ ձևավորող մարմին, ավելի է նպաստում քաղաքական համաձայնեցվածությանը, քան որոշումներ ընդունող որոշ մարմիններ: Տարբեր շահագրգիռ կողմերի անսովոր մեծ մասնակցությունը թուլացրեց ավանդական դարձած «ազդեցության ոլորտների համար պայքարը» և հնարավորություն տվեց շաղկապելու տարբեր նախաձեռնությունները համաձայնեցված քաղաքական մեկ գործընթացում: Այսպիսի մոտեցումը թույլ տվեց նաև մասնակիորեն լուծել կրկնապատկման հիմնախնդիրը, երբ տարբեր կազմակերպություններ, վերջին հաշվով, զբաղվում էին միևնույն հարցերի լուծմամբ:

7. Մշակեք ազգային, տարածաշրջանային և համաշխարհային մակարդակների միջև քաղաքականության մշակման գործուն փոխհարաբերություն

Ավելի ու ավելի փոխկապակցված աշխարհում դժվար է պահպանել միջազգային քաղաքականության ավանդական կառույցը, որը կազմված է տարածաշրջանային և համաշխարհային մակարդակներում միջազգային կազմակերպություններից: Ակնթարթային եռահաղորդակցությունը և ոչ պետական սուբյեկտների աճող ազդեցությունը ջնջում են քաղաքականության ազգային, տարածաշրջանային և համաշխարհային տարածությունների միջև սահմանը: Այս միասնական համաշխարհային քաղաքական տարածության մեջ հիմնախնդիրները «գաղթում են» մի մակարդակից դեպի մյուսը և մի հարթակից դեպի մյուս հարթակ: Նշանակալի դեր խաղացող, հատկապես ոչ պաշտոնական կազմակերպություններ օգտագործում են այդ հնարավորությունը, որպեսզի իրենց քաղաքական նախաձեռնությունները ներմուծեն ավելի նպաստավոր մակարդակում: ԵՄ երկրներում, օրինակ՝ կառավարությունները երբեմն օգտագործում են, այսպես կոչված, քաղաքականության լվացում՝ եթե նախաձեռնությունն ազգային մակարդակում չի ընդունվում, այն մտցվում է տարածաշրջանային մակարդակ և կրկին վերադարձվում է տվյալ երկիր, արդեն որպես « միջազգային պարտավորություն»: Համացանցի կառավարման բնագավառում քաղաքական ֆորումների ցանցը շատ բարդ է: Շատ տարբեր հարթակներ են գոյություն ունեցել մինչև IGF-ի ստեղծումը (միջազգային կազմակերպություններ, ICANN, Համացանցի միությունը, ստանդարտացման տարբեր մարմիններ): Բացի այդ, համացանցի կառավարման սուբյեկտները շատ դինամիկ են և ժամանակակից հեռահաղորդակցային տեխնոլոգիաների օգնությամբ

հանգիստ «գաղթում են» քաղաքականության մի մակարդակից կամ ֆորումից դեպի մյուսը: Համացանցի օգտագործմամբ կառավարման մասին ֆորումը փորձում է առավելագույնի հասցնել առավելությունները և կրճատել «բազմամակարդակ» քաղաքական գործընթացի ռիսկերը: Դրա շրջանակներում համաշխարհային, տարածաշրջանային և ազգային միջոցառումները համակարգվում են ինչպես «ներքևից վերև» (ֆորումին նախապատրաստվելու ընթացքում), այնպես էլ «վերևից ներքև» (ֆորումի աշխատանքների գործընթացում ստեղծված գիտելիքների տարածման ճանապարհով): IGF-ի բարձր թափանցիկությունը «հարմար» ֆորումի որոնումները և քաղաքական գործընթացների այլ մանիպուլյացիաները ավելի բարդ է դարձնում:
Ֆորումն այս տեսակետից թեև հասել է էական առաջխաղացման, սակայն դեռ շատ բան կա անելու:

8. Տարբեր մասնագիտական և կազմակերպչական մշակույթների միջև զարգացրեք հեռահաղորդակցությունը

Հարյուրավոր գրքեր են գրվել այն մասին, թե ինչպես պետք է շփվել տարբեր մշակույթներ ունեցող մարդկանց հետ՝ արաբների, ամերիկացիների և այլն: Սակայն IGF-ի փորձը ցույց էտալիս, որ քաղաքական գործընթացում հիմնական բարդությունը տարբեր մասնագիտական մշակույթների (օրինակ՝ իրավաբաններ, ինժեներներ) և տարբեր կազմակերպչական մշակույթների (օրինակ՝ միջազգային կազմակերպությունների, կառավարությունների, ընկերությունների) միջև հեռահաղորդակցային կապի հաստատումն է: Արդի համաշխարհայնացված աշխարհում հեռահաղորդակցության ակնթարթային կապի միջոցներին տիրապետելով, մեզ համար հաճախ ավելի հեշտ է շփվել մեկ մասնագիտական միջավայրի շրջանակներում, անտեսելով ազգային սահմանները: Օրինակ՝ ամերիկացի համակարգռային ինժեները կարող է զգալ, որ ավելի լավ փոխհարաբերություններ է ստեղծում չինացի ինժեների հետ, քան ամերիկացի դիվանագետի: Քանի որ համաշխարհային հարցերի տեխնիկական կողմի նշանակությունը մեծանում է (օրինակ՝ կլիմայի փոփոխությունն ու մարդու առողջությունը) միջմասնագիտական հեռահաղորդակցության արդյունավետության բարձրացումն ավելի կարևորվում է: Միջմասնագիտական շփման բարելավմանը կարելի է հասնել այլ մշակույթների հետ նախապատրաստման, կապի և ուսուցման միջոցով: Տարբեր մասնագիտությունների ներկայացուցիչների միջև առավել արդյունավետ շփումը նույնպես կարող է բարձրացնել տարբեր նախարարությունների և միջազգային կազմակերպությունների քաղաքականության համաձայնեցվածությունը:
Համացանցի կիրառմամբ կառավարման մասին ֆորումը նպաստեց միջմասնագիտական շփման հաստատմանը, ապահովելով տարբեր բնագավառների մասնագետների միջև գաղափարների արդյունավետ փոխանակում: Դրա վառ օրինակն է ֆորումի նիստերի մասնակիցների մասնագիտական և ինստիտուցիոնալ բազմազանությունը:

9.Խոստովանեք, որ տեխնիկական և գիտական հարցերը քաղաքականապես չեզոք չեն

IGF գործընթացը ցույց տվեց, որ յուրաքանչյուր տեխնիկական հարց ունի քաղաքական տեսանկյուն. այն ամրապնդում է որոշակի խմբերի դիրքորոշումները և առաջ է քաշում որոշակի շահեր: Մի որոշ փուլում տեխնիկական հարցերը վերածվում են քաղաքականի. քաղաքականության հարցերն, իրենց հերթին, պահանջում են որոշումներ ընդունել արժեքների և շահերի մասին:

Տեխնիկական հարցերը քաղաքական մակարդակում հայտնվում են նաև այլ բնագավառներում: Կլիմայի փոփոխման հարցերի վերաբերյալ Կոպենհագենում տեղի ունեցած բարձր մակարդակի հանդիպումը ցույց տվեց, որ ազգային պատվիրակությունների կազմում ավելի շատ լինելու են դիվանագետներ և քաղաքագետներ ու ավելի քիչ կլիմայի փոփոխման հիմնախնդրում մասնագիտացված գիտնականներ: Քանի որ դիվանագիտական գործընթացներն ավելի ու ավելի են հատվում գիտության և տեխնիկայի ոլորտները, այդ երկու ոլորտների սահմանազատման հարցի հրատապությունը աճելու է:

10. Հիշեք, որ տեքստը դիվանագիտության համար մնում է կարևոր

Չնայած վիրտուալ համաժողովների և այլ տեխնոլոգիաների ներուժին, այսօր առավել շատ, քան նախկինում, տեքստը դիվանագիտության կարևոր գործիքն է մնում1: Տեքստը գլխավոր տեղ է գրավում IGF գործընթացում, չնայած այն բանին, որ ֆորումի գործունեության արդյունքը որևէ պաշտոնական փաստաթուղթ չէ (օրինակ՝ պայմանագիր կամ հռչակագիր): Նախապատրաստական նիստերի արանքում շփումն իրականացվում է հիմնականում էլեկտրոնային փոստով և հասցեատերերի ցուցակների միջոցով: IGF-ի կայքը հագեցած է տեքստերով, դրանում համեմատաբար քիչ են լուսանկարները կամ պատկերները: Տեքստը կարևոր է նաև գործունեության երկու այլ ձևերի համար, որոնք առանձին քննարկվում են ստորև՝ սղագրված հաշվետվություններ և հեռավոր մասնակցություն: IGF-ի փորձը ցույց է տալիս, որ գործընթացների բազմակողմանի բնույթը տեքստի նշանակությունը չի նվազեցնում: Իրականում ակնհայտ դարձավ, որ հիմնական գործընթացները պետք է կառուցվեն տեքստի շուրջ: Այս փաստը պետք է արտացոլված լինի համաշխարհային քաղաքական գործընթացներին մասնակցելու շահագրգիռ կողմերի ուսուցման և նախապատրաստման գործում:

11.Գնահատեք բառացի հաշվետվությունների ազդեցությունը դիվանագիտության վրա

Բառացի հաշվետվությունները իրական ժամանակում՝ ժողովի ընթացքում բանավոր հայտարարությունների ներկայացումն ու գրանցումն է, ինչը ընթացակարգային և տեխնիկական նորարարություն է, որը կարող է էական ազդեցություն ունենալ այն բանի վրա, թե ինչպես է իրականացվում

բազմակողմանի դիվանագիտությունը: ICANN փորձի հիման վրա, համացանցի կառավարման աշխատանքային խմբի քարտուղարությունը (WGIG) 2005 թ. ապրիլին սկսեց ներկայացնել բառացի հաշվետվություններ: Այդ փորձը շարունակվեց IGF-ի ընթացքում, իսկ վերջերս ներդրվել է նաև ՀՄՄ-ում: Բանավոր բոլոր հաշվետվությունները գրառում են իրական ժամանակում հատուկ սցագրողները և անմիջապես դրանք երևում են նիստերի դահլիճում տեղադրված մեծ էկրանին, ինչպես նաև փոխանցվում է համացանցի միջոցով: Պատգամավորների ելույթների ժամանակ էկրանի վրա ներկայացվում են նրանց ելույթները:
Բառացի հաշվետվությունները նշանակալիորեն ազդել են այն բանի վրա, թե ինչպես է իրականացվում դիվանագիտությունը , դրա modus operandi-ի վրա: Այն գիտակցումը, որ ասելիքը պահվելու է գրավոր ձևով, շատ պատգամավորների ստիպում է զգույշ լինել բանավոր ելույթի տևողության և մակարդակի ընտրության հարցում: Բանավոր հաշվետվությունները բարձրացրին նաև դիվանագիտական բանակցությունների թափանցիկությունը:

12.Բարձրացրեք բացախոսությունն ու ներկայացուցչությունը՝ հեռակառավարվող մասնակցության կենտրոնների օգնությամբ

IGF-ի հիմնական նպատակներից մեկը գործընթացին տարբեր երկրների և շահագրգիռ խմբերի մասնակցության ապահովումն է: Համացանցի կառավարմանը նվիրված ֆորումի համար բնական կլիներ համացանցն օգտագործել IGF բոլոր հանդիպումներում մասնակցություններն ընդլայնելու համար՝ դրանց մասնակցելու թույլտվություն տալով նույնիսկ նրանց, ովքեր չեն կարողացել ֆիզիկապես ներկա գտնվել: Աթենքում տեղի ունեցած առաջին բանակցությունների ընթացքում ֆորումի քարտուղարությունը ապահովել էր ինչպես նախապատրաստական, այնպես էլ հիմնական միջոցառումների տեսա, ձայնա և տեքստային հաղորդումները: Այդ նյութերը հիմնականում դիտում էին նրանք, ովքեր հետաքրքրվում էին IGF-ով: Արդյունքում հեռավոր մասնակցության մակարդակը համեմատաբար համեստ էր և թույլ չտվեց գործընթացում ընդգրկել IGF-ում քննարկվող թեմաներով հետաքրքրվող բոլոր կողմերին: Որպես լուծում առաջարկվեց կիրառել «հեռավոր կենտրոնները» («հաբեր»): Դրանց ներքո ընկալվում են տեղում կազմակերպվող հանդիպումները, որոնք անցկացվում են IGF նիստերի ընթացքում և դրանց զուգահեռ: Այդպիսի հանդիպումների կազմակերպիչներն են համալսարանները, ՏՀՏ կենտրոնները, ոչ կառավարական կազմակերպությունները և այլ խմբեր ու միավորումներ, որոնք զբաղվում են համացանցի կառավարման հարցերով: Հանդիպումների շրջանակներում կազմակերպվում է IGF նիստերի հաղորդում, որպեսզի հեռու գտնվող մասնակիցները տեղյակ լինեն տվյալ պահին քննարկվող հարցի մասին: Նրանք նաև կարող են ուղարկել տեքստային և տեսագրված հարցեր, որոնց IGF քննարկման մասնակիցները պատասխանում են «ուղիղ եթերով»: Բացի այդ, «հեռավոր կենտրոնները» հավաքում են փորձարարական

խմբեր և կազմակերպում կլոր սեղաններ, որոնց ընթացքում IGF թեմաները քննարկվում են տեղական իրականությունը հաշվի առնելով: Այդ գործունեության շրջանակներում հեռավոր կենտրոնները թույլ են տալիս ավելի արդյունավետորեն համակարգել քաղաքական գործընթացները համաշխարհային ու տեղական մակարդակով: Օրինակ՝ 2008 թ. IGF-ի ընթացքում կենտրոնը Մադրիդում ցույց էր տալիս նիստերը և կազմակերպում էր Իսպանիայի հանդեպ կիրառվող կիբեռանվտանգության հարցերի վերաբերյալ քննարկումներ: IGF-ին զուգահեռ 2008 թ. ընդհանուր առմամբ աշխատում էր ութ հեռավոր ցանց (Մադրիդ, Լախոր, Բարսելոն, Բելգրադ, Բուենոս Այրես, Սան Պաուլու, Բոգոտա և Պունա): Չորս օրվա ընթացքում ավելի քան 450 ժամ ցուցադրվել են միջոցառումները, քննարկումներին մասնակցել են հեռակառավարման 522 այցելու3: 2008 թ. հաջողությամբ տեստավորելուց հետո, հեռավոր կենտրոնների հայեցակարգն ընդունում է IGF քարտուղարությունը: Սպասվում է, որ հեռակառավարվող մասնակցությունը նշանակալիորեն կընդլայնվի 2009 թ. Շարմ էշ Շեյխում տեղի ունեցող հաջորդ IGF-ի ընթացքում3:

Համացանցի կառավարման ֆորումի փորձը ցույց է տալիս, որ հեռակառավարվող մասնակցությունը զգալիորեն ավելացնում է միջազգային խորհրդակցությունների բացախոսությունը և տարբեր հետաքրքրությունների ներկայացվածությունը, նպաստում է համաշխարհային և տեղական քաղաքական ասպարեզների միջև կապի ձևավորմանը, ինչը հաճախ բացակայում է միջազգային դիվանագիտության մեջ:

3. Այս գրքի տեքստը պատրաստվել է 2009 թ. աշնանը՝ մինչ Շարմ էշ Շեյխում ֆորումի անցկացումը:

13. Հաշվի առեք պաշտոնական արձանագրության (կամ դրա բացակայության) և հավասար մասնակցության միջև կապը

IGF-ի առջև ծառացած հիմնախնդիրներից մեկը ՄԱԿ-ի աշտոնական դիվանագիտության մշակույթի և համացանցային միության ոչ պաշտոնական մշակույթի հակադրությունն է: Ֆորումի ամենամյա երեք հանդիպումներից հետո, կարծես, ոչ պաշտոնական մշակույթը հաղթանակել էր: Թեև այդ մշակույթը ստեղծում է ներառելու մթնոլորտ, նպաստում է երիտասարդության և տարբեր միությունների մասնակցությանը աշխարհով մեկ, այնուամենայնիվ այն կարող է որոշ հիմնախնդիրների աղբյուր լինել: Ոչ պաշտոնական իրավիճակում սոցիալական հիերարխիայի հանդեպ հարգանքն ընդգծող մշակույթ ունեցող երկրներից մասնակիցները կարող են իրենց հարմարավետ չզգալ և քննարկումներում իրենց ավանդը չնրդնել: Բացի այդ, դիվանագիտական, իրավական և այլ մասնագիտական մշակույթներում քննարկումներին մասնակցությունը կառուցված է մասնագիտական արձանագրություններով: Այդ պատճառով աշխատանքային գործընթացի և քննարկումների ոչ պաշտոնական լինելը կարող է խոչընդոտել որոշ պատգամավորների մասնակցությանը

և դառնալ անհավասարության աղբյուր: IGF-ը պատասխանում է այդ ռիսկերին, միջոցներ գտնելով զուգադրելու տարբեր մակարդակի ձևականությունները, առաջարկելով աշխատանքի մի քանի ձևաչափեր, որոնցում բոլոր շահագրգիռ կողմերը կարող են մասնակցել՝ չզգալով անհարմարավետություն: Օրինակ՝ IGF-ը բարձրացրել էր որոշ՝ հիմնականում լիակազմ նիստերի արձանագրությունների ձևի մակարդակը, մտցնելով դիվանագիտության համար ավելի տիպիկ ընթացակարգերի կանոններ (օրինակ՝ ելույթների, հարցերի տրման կարգը) և կազմակերպել էր հատուկ նիստեր՝ խորհրդարանականների համար:

14. Ապահովեք զարգացող երկրների արդյունավետ մասնակցությունը. ձևական հավասարությունից գործառնականին անցումը

ՄԱԿ-ի կառուցվածքներում փոքր և զարգացող պետությունները ապահովում են իրենց համար, սովորաբար հավասար կարգավիճակ են ապահովում՝ պնդելով ներկայացուցչության պաշտոնական սկզբունքներն ու ընթացակարգերը: Ի տարբերություն խոշոր և զարգացած պետությունների, փոքր և զարգացող երկրները չունեն բիզնեսի, քաղաքացիական հասարակության և ակադեմիական շրջանակների ընդհանուր ուժերով հասարակության շահերը զուգահեռ ներկայացնելու համար ցանց: Այդ պատճառով էլ զարմանալի չէ, որ նրանք կարող ենք անվստահորեն վերաբերվել ոչ պետական տարբեր սուբյեկտների մասնակցությանը: «Մեծ մասշտաբի» նիստերի ժամանակ, որտեղ հավասար իրավունքների հիմունքներով հավաքվում են հազարավոր մասնակիցներ, այն կորցնում է ՄԱԿ-ի ընթացակարգերի «պահպանումը», որի համաձայն 194 պետությունների բոլոր մասնակիցներն ունեն պաշտոնապես հավասար կարգավիճակ՝ անկախ նրանց մեծության չափից և հզորությունից:
2002 թ. տեղեկատվական հասարակության (WSIS) բարձր մակարդակի համաշխարհային հանդիպման նախապատրաստական գործընթացի սկզբում փոքր և զարգացող երկրներից շատերը վճռականորեն հանդես եկան քաղաքացիական հասարակության և գործարար շրջանակների ներկայացուցիչների հավասար իրավունքներով մասնակցության մասին արված առաջարկության դեմ: Այդ պետություններից մի քանիսը համացանցի կառավարման հարցերում «միասնական պատուհանի» սկզբունքին կողմ արտահայտվեցին, ինչը նրանց կարող էր տալ մեկ, միջկառավարական նախընտրելի «հարթակ»՝ համացանցի կառավարման բոլոր հարցերը քննարկելու համար4: 2002 թ.-ից սկսած WSIS-ը, WGIG-ը և հատկապես IGF-ը մեծ առաջընթացի են հասել բազմակողմանի գործընթացի ասպեկտների զարգացման ամրապնդմանն ուղղված գործում, այդ թվում նաև ապահովելով փոքր և զարգացող պետությունների բավարար քանակի ներկայացուցչությունը:
1. Պաշտոնական մակարդակով IGF -ը երաշխավորում է, որ զարգացող երկրների տարբեր շահագրգիռ կողմերը համապատասխանորեն

ներկայացված են բոլոր նիստերին և փորձարարական խմբերում: Զարգացող երկրների մասնակցության մակարդակի բարձրացումն ակնհայտ է Ռիո դե Ժանեյրոյում և Հայդարաբադում տեղի ունեցած հանդիպումների օրինակներում:

2. IGF-ի գործընթացը օգնեց փոքր և զարգացող շատ պետությունների ավելի արդյունավետ օգտագործել մարդկային ռեսուրսները: Խոսքը ոչ միայն դիվանագետների մասին է, այլև այլ քաղաքացիների, ովքեր փորձ ունեն համացանցի կառավարման բնագավառում, աշխատում են ողջ աշխարհի համացանցի հետ կապված կազմակերպություններում և համալսարաններում: Փոքր պետությունների համար առանձնահատուկ կարևորություն ունի արտասահմանում աշխատող փորձագետների ներուժի օգտագործումը:

3.Ֆիզիկական մասնակցությունը, այսինքն՝ նիստերին ներկա գտնվելը դեռ չի նշանակում հավասար մասնակցություն: Այն յուրաքանչյուր մասնակցից պահանջում է համապատասխան գիտելիքներ, հմտություններ և քաղաքական գործընթացին մասնակցելու համար ինքնավստահություն: IGF-ը փորձում էր ապահովել հավասար մասնակցություն՝ ներուժի զարգացմանն ուղղված միջոցառումների միջոցով: 2002 թ. սկսած զարգացող և փոքր երկրներից ավելի քան 1000 պաշտոնատար անձինք և մասնագետներ ներգրավվել էին ներուժի զարգացմանն ուղղված կադրերի պատրաստման և այլ միջոցառումներում: Այդ միջոցառումները դուրս էին ավանդական ակադեմիական դասընթացների շրջանակներից, ապահովում էին ուսուցման, քաղաքականության բնագավառում հետազոտությունների և քաղաքականության գործընթացին լծվելու բացառիկ համադրությունը, որպեսզի մասնակիցներին օգնեն հասկանալու IGF-ի դինամիկան և ձեռք բերեն քաղաքական գործընթացներում լիարժեքորեն ու արդյունավետորեն մասնակցելու համար անհրաժեշտ ինքնավստահություն: Ուսուցման գործընթացում տարբեր շահագրգիռ կողմերի ներգրավումը (դիվանագետների, չինովնիկների, ինժեներների) մասնակիցներին թույլ տվեց հասկանալու բազմակողմանի մոտեցման առավելությունը, տվեց անհրաժեշտ վստահություն՝ այլ մասնագիտական միությունների ներկայացուցիչների հետ բանակցություններին մասնակցելու համար:

4. IGF գործընթացը նպաստեց նաև համացանցի կառավարման բնագավառում «պրակտիկայի միությունների» զարգացմանը «համաշխարհային հարավում», ինչպես տարածաշրջանային (օրինակ՝ Արևմտյան Աֆրիկա, Արևելյան Աֆրիկա, Լատինական Ամերիկա), այնպես էլ ազգային մակարդակով (օրինակ՝ Քենիա, Բրազիլիա, Սենեգալ): Այդ միությունները օգնեցին փոքր և զարգացող շատ պետությունների գործընթացի մեջ ներգրավելու տարբեր շահագրգիռ կողմերի, ոչ կառավարական շրջանակներում բացահայտելով փորձագետների, որոնք արդեն մասնակցում են գիտական հետազոտություններում և համացանցի կառավարման գործընթացին:

Ընդլայնելով մասնակցության մասշտաբը, խրախուսելով ներուժի

զարգացումը և աջակցելով միությունների ու ցանցերի ստեղծմանը, IGF-ը օգնեց զարգացող երկրներին համացանցի կառավարման հարցում պաշտոնական պասսիվ մասնակցությունից անցնելու ակտիվ գործառնականի:

Ծանոթագրություններ

1.Հետաքրքիր զուգահեռ կարելի է անցկացնել բջջային հեռախոսների SMS ծառայությունների կիրառման հետ. տեքստի գոյությունը նախկինի պես անհրաժեշտ է մարդկային շփման համար, անկախ տեսա և ձայնահաղորդման հզոր գործիքների առկայությանը:

2. Այդ կետի վերաբերյալ արժեքավոր և բովանդակալից նկատառումներ են ներկայացրել Ջինջեր Պակը (Ginger Paque) և Մարիլիա Մարսելը (Marilia Marcel)՝ հեռավոր մասնակցության աշխատաքային խմբի ակտիվ անդամները (www.igfremote.com):

3. IGF-2008-ում հեռավոր մասնակցության վերաբերյալ մանրամասն հաշվետվությունը հասանելի է համացանցային հետևյալ հասցեում՝ http://www.igfremote.com/ReportRPIGF-fi nal.pdf:

4. Նախնական ուսումնասիրությունները ցույց են տալիս, որ համացանցի կառավարման տարբեր տեսանկյուններով զբաղվում են 80-100 միջազգային կազմակերպություններ, ստանդարտացման հարցերով զբաղվող մարմիններ, ֆորումներ և այլ կազմակերպություններ: Նույնիսկ խոշոր զարգացած պետությունների համար համարյա անհնար է գրավել այսքան մեծ դաշտ: IGF-ը փորձում էր նվազեցնել այդ բարդությունը՝ «զտելով» համացանցի կառավարման հարցերը քաղաքական այլ հարցերից (մասնավոր կյանքի գաղտնիք, մտավոր սեփականություն, մարդու իրավունքներ, զարգացում, էլեկտրոնային առևտուր և այլն):

Հավելված 3

Համացանցի կառավարման զարգացման ամփոփում

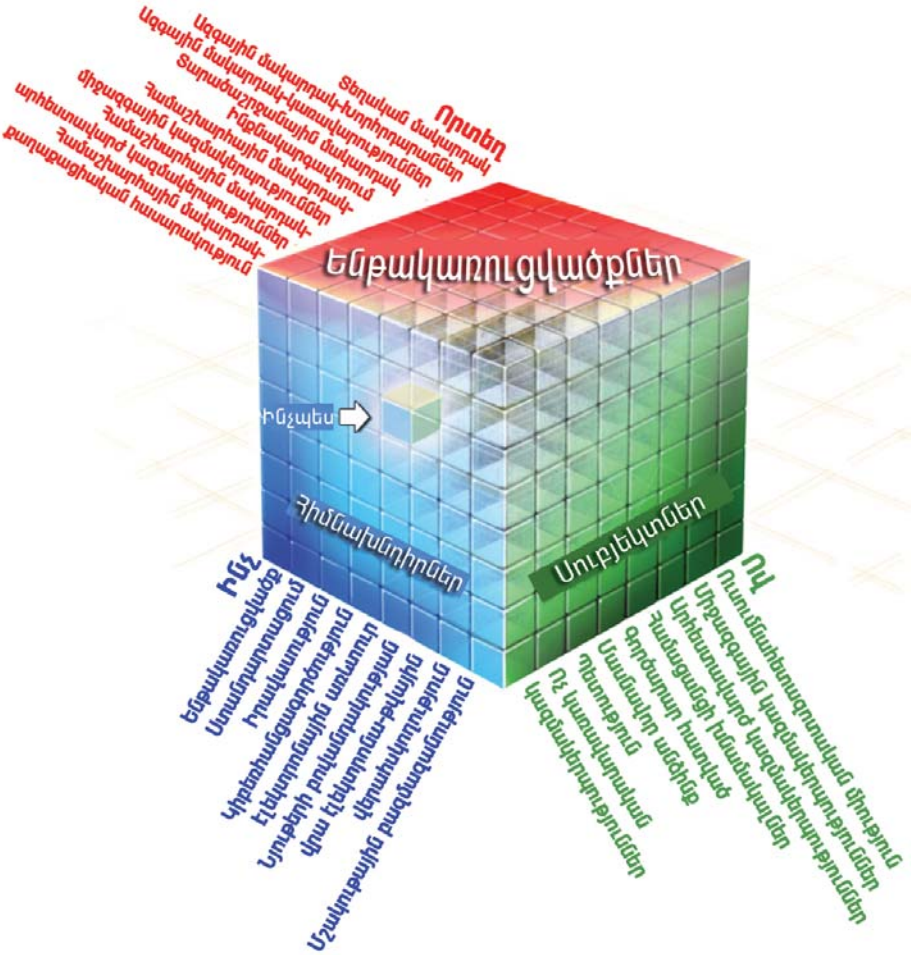
Գործող անձ / Ժամանակա-շրջան	ԱՄՆ	Համա-ցանցի «խնամա-կալները»	Միջազգային կազմակեր-պություններ	Մասնավոր հատված	Պետություն	Քաղաքա-ցիական հասարա-կություն
	Պաշտպանության նախարարությունը կառավարում է DNS համակարգը					
1986	Գիտության ազգային հիմնադրամը (ԳԱՀ) պաշտպանության նախարարությունից ընդունում է համացանցի կառուցվածքների կառավարումը					
1994				NSI ընկերությունը ԳԱՀ-ի հետ պայմանագիր է կնքում 1994–1998 թթ. DNS համակարգի կառավարման մասին		
«DNS պատերազմի» սկիզբը DNS-ի կառավարումը ԳԱՀ-ից NSI-ին (մասնավոր ընկերությանը) փոխանցելուց հետո համացանցային ընկերությունը (առաջին հերթին՝ ISOC) երկար տարիներ փորձում էր DNS կառավարումը վերադարձնել հասարակական վերահսկողությանը: Չորս տարի անց դա նրան հաջողվում է: Ստորև բերվում է այդ գործընթացի ամփոփումը, որն ընդգրկում է բազում դիվանագիտական հնարքներ՝ բանակցություններ, կոալիցիայի ստեղծում, ուժի գործադրում, համաձայնություն գտնել և այլն:						
1996 թ. հունիս		IANA/ISOC-ը ծրագրում են պայմանագրի ավարտից հետո ստանձնել NSI-ի գործառույթները: Ի հայտ են գալիս նոր դոմեններ, նոր դոմենների դեմ ՀՄՄ-ի և առևտրային ապրանքանիշերի պահպանման հարցում շահագրգիռ մասնակիցների ուժեղ ընդդիմությունը:				
1997 թ. գարուն		Միջազգային հատուկ կոմիտեի (ՄՀԿ– International Ad Hoc Committee) ստեղծման մասին առաջարկություն: ՄՀԿ մասնակցեր. շահեր ունեցող խմբերից երկուական ներկայացուցիչ (ապրանքանիշերի պահպանման ոլորտում), ՀՄՄ, ՄՀԿ և ԳԱՀ. և հինգ ներկայացուցիչ IETF-ից: Բարձր մակարդակի արմատական դոմենային անունների փոխըմբռնման մասին հուշագրի ստորագրում, որը նախատեսում է՝ DNS-ի՝ որպես «հասարակական ռեսուրսի» կարգավիճակը, յոթ նոր դոմենների ստեղծում, ապրանքանիշերի պահպանման ամրապնդում: Արձանագրողների խորհրդի ստեղծում (Council of Registers)՝ ստորագրման արարողությունը տեղի է ունեցել Ժնևում, 1997 թ. մարտին, ՀՄՄ-ում: Արձանագրողների խորհուրդն անմիջապես լուծարվեց: ԱՄՆ կառավարության, ԳԱՀ-ի և Եվրամիության հզոր ընդդիմությունը:			
1997	ԱՄՆ կառավարությունը DNS-ի կառավարումը փոխանցում է առևտրի նախարարությանը					

Գործող անձ / Ժամանակաշրջան	ԱՄՆ	Համացանցի «խնամակալները»	Միջազգային կազմակերպություններ	Մասնավոր հատված	Պետություն	Քաղաքացիական հասարակություն
1998 թ. հունիս	Առևտրի նախարարության «Սպիտակ գիրքը» կոչ է անում հիմնական մասնակիցներին սեփական առաջարկներն անել	Առաջարկություններ են լինում «Սպիտակ գրքին» նվիրված միջազգային ֆորումից (International Forum on White Paper), Արմատական սպասարկուների բաց կոնֆեդերացիայից (Open Root Server Confederation) և Բոստոնի աշխատանքային խմբից (Boston Working Group):				
		ISOC նոր փաստաթղթի նախապատրաստման փոխարեն կենտրոնանում են՝ - խոշոր կոալիցիայի ստեղծման վրա, որն ընդգրկելու է՝ միջազգային կազմակերպություններ (ՄՀԿ նախաձեռնությունը), մասնավոր հատվածի ներկայացուցիչներին (IBM) և առանցքային երկրներին (ԵՄ, Ճապոնիա, Ավստրալիա), -նոր կազմակերպության ստեղծման վրա:				
1998 թ., երկրորդ կես		1998 թ. սեպտեմբեր- ISOC և NSI միջև նախնական համաձայնագիր 1998 թ. հոկտեմբեր- ISOC-ը հեղյալ է հայտարարում համաձայնագիրը և ստեղծում է ICANN				
1998 թ. նոյեմբերի 15	առևտրի նախարարությունը իր լիազորությունները հանձնում է ICANN-ին:	ICANN-ը ստանում է երկու կարևոր նոր գործառույթներ՝ - բարձր մակարդակի արմատական դոմեններ արձանագրողներին հավատարմագրեր տալու իրավունք, - հիղինակության վրա հիմնված կառավարում (քաղաքական տեսակետը, նախկինի պես, վերահսկում է ԱՄՆ առևտրի նախարարությունը):				
1999 թ. ապրիլ		ԱՄՆ, ICANN և NSI միջև համաձայնագիր ու «համընդհանուր օգտագործման գրանցման համակարգի» ներդրում (shared registry system): NSI-ը կորցնում է մենաշնորհը, սակայն ձեռք է բերում անցումային շրջանի համար նպաստավոր պայմաններ (չորս դոմենի կառավարում):				
ICANN-ի կառուցվածքը և գործառույթները						
1998 թ. հունիս		Արձանագրությունների աջակցման կազմակերպության ստեղծում (Protocol Supporting Organization), որն ընդգրկում է IETF, W3C և համացանցի այլ «պիոներներին»	ՄՄՀԿ շրջանակներում սկսվում է «համացանցի դոմենային անունների» գործընթաց	Ստեղծված է Հասցեների աջակցման կազմակերպություն (Address Support Organization), որպեսզի ներկայացվի DNS (ARIN, RIPE, NCC) արձանագրողների ընկերակցությունը: Ստեղծված է դոմենային անունների աջակցման կազմակերպություն (Domain Name Supporting Organization)՝ ապրանքանիշերի և առևտրային շահերի պաշտպանության համար:	30 երկիր միասին ստեղծում են կառավարության խորհրդակցական կոմիտե (Government Advisory Committee), որպեսզի ավելի մեծ ազդեցություն ձեռք բերեն ազգային դոմենների վրա: Ի պատասխան դրա ICANN-ը ստեղծում է երկրների բարձր մակարդակի դոմենների ենթակոմիտե:	
«DNS պատերազմի» ավարտը «Պատերազմ» ավարտվեց փոխզիջումներով: ISOC-ին հաջողվում է DNS կառավարման վրա ընդլայնել հասարակական վերահսկողությունը, թեև առևտրային շահերը դեռևս շատ ուժեղ են: Այսպիսով, պաշտպանվում են և՛ մասնավոր բիզնեսի, և՛«իսնամակալների» շահերը: Սակայն պետությունների և համացանցային միությունների դիրքորոշումների առումով այդպես չէ: Դրանք ICANN կառավարման համակարգի առավել թույլ կողմերն են:						
2000–2003			Համացանցն ավելի ու ավելի է գրավում ՀՄՄ-ի, ՄՄՀԿ-ի, ՅՈՒՆԵՍԿՕ-ի, ՏՀԶԿ-ի, ԵԽ-ի և համաշխարհային բանկի ուշադրությունը:	Մասնավոր հատվածն ուժեղ ճնշում է գործադրում հոգուտ համացանցի կառավարման (հեղինակային իրավունքի պաշտպանություն, էլեկտրոնային առևտուր և այլն):	Համացանցին վերաբերող օրենսդրության և դատական գործի զարգացում:	Ոչ կառավարական կազմակերպությունները ներգրավվում են «թվային զարգացման», մարդու իրավունքների, համացանցում գենդերային հիմնախնդիրների լուծման գործում:

Գործող անձ / Ժամանակաշրջան	ԱՄՆ	Համացանցի «խնամակալները»	Միջազգային կազմակերպություններ	Մասնավոր հատված	Պետություն	Քաղաքացիական հասարակություն
			Համացանցի զարգացմանն ու կառավարմանը նվիրված բազմահատված և համաշխարհային նախաձեռնություններ և այլն: «Մեծ ութնյակի» թվայնացման հնարավորությունների գծով նպատակային խումբ (G-8 Dot Force), Համաշխարհային տնտեսական ֆորում, ՏՀՏ-ի գծով ՄԱԿ-ի նպատակային խումբ, Հանուն գիտության համաշխարհային գործընկերություն:			
2002 թ. հունիս - 2003 թ. նոյեմբեր	2002 թ. հունիսին տեղի ունեցավ WSIS-ի առաջին նախապատրաստական հանդիպումը, Բեյրութի և Արևմտյան Ասիայի տարածաշրջանային նախապատրաստական հանդիպման ժամանակ (2003 թ. հունվար) համացանցի կառավարման հարցը մտցվեց օրակարգ: WSIS մասնակիցները Ժնևում համացանցի կառավարման հարցը ընդգրկում են հանդիպման թունիսյան փուլի օրակարգում (2005 թ.): Բազմահատվածային և համաշխարհային նախաձեռնություններ՝ նվիրված համացանցի զարգացմանը. «Մեծ ութնյակի» Dot Force խումբ, Համաշխարհային տնտեսական ֆորում, ՏՀՏ հարցով ՄԱԿ-ի նպատակային խումբ:					
2004-2005 թթ.	Այս ժամանակահատվածում համացանցի կառավարման վերաբերյալ քննարկումների բովանդակությունը տալիս էր համացանցի կառավարման աշխատանքային խումբը (WGIG): WGIG-ն ընդգրկում էր տարբեր շահագրգիռ կողմերի՝ կառավարությունների, գործարար և քաղաքացիական հասարակության ներկայացուցիչների: WGIG-ը անցկացրել է նախապատրաստական չորս հանդիպում և պատրաստել էր հաշվետվություն, որը դարձավ Թունիսում (2005 թ.) WSIS հանդիպման ժամանակ համացանցի կառավարման վերաբերյալ հետագա որոշումների հիմքը: WSIS-ի մասնակիցները Թունիսում որոշում են ստեղծել համացանցի կիրառմամբ կառավարման վերաբերյալ ֆորում՝ որպես արդյունք ICANN-ի վրա հիմնված կարգում ցանկացած փոփոխության հակառակորդների և համացանցի կառավարման միջպետական կարգի կողմնակիցների միջև փոխզիջման:					
2006–2009 թթ.	WSIS (2005 թ.) թունիսյան փուլի ավարտից հետո համացանցի կառավարման քաղաքական գործընթացի շարունակման նպատակով ստեղծվում է համացանցի կիրառմամբ կառավարման ֆորում (IGF): Մինչ օրս տեղի են ունեցել ֆորումի չորս հանդիպում՝ 2006 թ. Աթենքում, 2007 թ. Ռիո դե Ժանեյրոյում, 2008 թ. Հայդարաբադում, 2009 թ. Շարմ էշ Շեյխում: 2009 թ. սեպտեմբերի 30-ին ԱՄՆ կառավարությունը և ICANN-ը ստորագրում են «Պարտականությունների հաստատումը»: Այս փաստաթուղթը վերջ է դնում ICANN-ի վրա ԱՄՆ վերահսկողությանը, որը համացանցի կառավարման ամենավիճելի պահերից մեկն էր: ICANN-ը արդեն որպես անկախ կազմակերպություն նոր փուլ է մտնում: Ներկայում նրա հետագա կարգավիճակի և դերի մասին հարցերն ավելի շատ են, քան պատասխանները:					
2010	Համացանցի կառավարման հինգերորդ ֆորումը կանցկացվի Վիլնյուսում: Ամփոփելով անցած հինգ տարիների արդյունքները՝ 2010 թ. աշնանը ՄԱԿ-ը որոշում կկայացնի IGF-ի ապագայի վերաբերյալ:					

Հավելված 4

Համացանցի կառավարման խորանարդը



«Ինչ» առանցքը վերաբերում է այն հարցերին, որոնք քննարկվում են համացանցի կառավարման շրջանակներում (ենթակառուցվածք, հեղինակային իրավունք, մասնավոր կյանքի գաղտնիք և այլն): Այն տվյալ մոտեցման բազմակարգապահության մարմնավորումն է:
«Ինչ» առանցքում ներկայացվում են հիմնական գործող անձինք

(պետություն, միջազգային կազմակերպություններ, քաղաքացիական հասարակություն, մասնավոր սեկտոր): Այս կողմը ներկայացնում է գործընթացի բազում մասնակիցների (բազմակողմանի մոտեցում): «Որտեղ» առանցքը բնութագրում է այն կառուցվածքները, որի շրջանակներում կարող են լուծվել համացանցին վերաբերող հարցերը (ինքնակարգավորում, տեղական, ազգային, տարածաշրջանային և համաշխարհային մակարդակների): Սա համացանցի կառավարման բազմամակարդակ մոտեցման պատկերն է:
Խորանարդի երեք առանցքները միմյանց հատվելով, ձևավորում են յուրօրինակ խաչմերուկներ, որոնցից յուրաքանչյուրին կարելի է տալ «Ինչպե՞ս» հարցը: Այդպիսի խաչաձևումից յուրաքանչյուրն օգնում է հասկանալ թե ինչպես պետք է կարգավորել այս կամ այն հարցը և՛ իրավաճանաչողական տեխնոլոգիաների, և՛ գործիքակազմի («փափուկ իրավունք», պայմանագրեր, հռչակագրեր) տեսանկյունից: Այդպիսի խաչաձևումներից մեկն օգնում է հասկանալ, թե ինչպես քաղաքացիական հասարակությունը (ով) ազգային մակարդակում (որտեղ) պետք է գործի մասնավոր կյանքի գաղտնիքին վերաբերող (ինչ) հարցերի նկատմամբ: Խորանարդից դուրս քննարկվում է «երբ» բաղադրամասը:

DiploFoundation

DiploFoundation-ն ոչ առևտրային կազմակերպություն է, որի նպատակն է օգնել շահագրգիռ բոլոր կողմերին մասնակցելու դիվանագիտությանը և միջազգային հարաբերությունների գործընթացին: Մեր գործունեության հիմնական ուղղություններն են՝ կրթությունը, մասնագիտական պատրաստությունը և ներուժի զարգացումը:

Դասընթացներ- Մենք հետդիպլոմային մակարդակի դասընթացներ և լայն շրջանակի կրթական սեմինարներ ենք առաջարկում բոլոր նրանց, ովքեր կապ ունեն դիվանագիտության հետ:

Մեր լսարանը՝ դիվանագետներ, պետական ծառայողներ, միջազգային և ոչ կառավարական կազմակերպությունների աշխատակիցներ, ինչպես նաև բոլոր նրանք, ովքեր ուսումնասիրում են միջազգային հարաբերությունները: Դասընթացներն առաջարկվում են առցանց ձևաչափով կամ «խառը» ուսուցում (առցանց և ցանցից դուրս):

Ներուժի զարգացում- Մեր հովանավորների և գործընկերների օգնությամբ մենք զարգացող երկրների համար առաջարկում ենք ներուժի զարգացման ծրագրեր այնպիսի թեմաներով, ինչպիսիք են՝ համացանցի կառավարումը, մարդու իրավունքները, հանրային դիվանագիտություն, դիվանագիտությունը առողջապահության բնագավառում:

Հետազոտություններ- Հետազոտական նախագծերի և համաժողովների շրջանակներում մենք ուսումնասիրում ենք դիվանագիտության, միջազգային հարաբերությունների և առցանց ուսուցման վերաբերյալ հարցեր:

Հրապարակումներ- Մեր հրապարակումները նվիրված են ինչպես արդի միտումներին, այնպես էլ դիվանագիտության ավանդական տեսակետների նորովի իմաստավորմանը:

Ծրագրային ապահովման մշակում- Մենք մշակել ենք մի շարք ծրագրային հավելվածներ՝ հատուկ դիվանագետների և միջազգային հարաբերությունների այլ մասնագետների համար: Մեր ուժեղ կողմերից է նաև առցանց ուսուցման համար հարթակի մշակումը:

Diplo կենտրոնական գրասենյակը գտնվում է Մալթայում, իսկ երկու այլ գրասենյակներ՝ Ժնևում և Բելգրադում: Diplo-ն ի հայտ է եկել դիվանագիտության մեջ տեղեկատվահեռահաղորդակցային տեխնոլոգիաների ներդրման նախագծից, որը սկսվել է 1993 թ., Մալթայի դիվանագիտական հետազոտությունների միջերկրածովյան ակադեմիայում: 2002 թ. նոյեմբերին Diplo-ն ձեռք է բերում ոչ առևտրային անկախ ֆոնդի կարգավիճակ, որի հիմնադիրներն են Մալթայի և Շվեյցարիայի կառավարությունները: Մեր գործունեության շրջանակն ընդլայնվել է դիվանագիտության ասպարեզում և այսօր ընդգրկում է դիվանագիտության ու միջազգային հարաբերությունների ուսուցման և գործի ինչպես նոր, այնպես էլ ավանդական կողմերը:

Հեղինակի մասին

Յովան Կուրբալիան DiploFoundation հիմնադրամի հիմնադիրն ու տնօրենն է: Նախկինում արհեստավարժ դիվանագետ լինելով, նա իրավական, դիվանագիտության և տեղեկատվական տեխնոլոգիաների բնագավառներում աշխատանքի և ուսումնասիրությունների մեծ փորձ ունի:

1992թ. Կուրբալիան Մալթայի Միջերկրածովյան ակադեմիայում ստեղծել է տեղեկատվական տեխնոլոգիաների և դիվանագիտության կենտրոն: Ուսուցման, հետազոտությունների և հրապարակումների բնագավառում ավելի քան տասը տարվա բեղմնավոր աշխատանքից հետո, 2003 թ. կենտրոնը վերածվում է DiploFoundation հիմնադրամի: 1994 թ. դոկտոր Կուրբալիան դասընթացներ է անցկացրել դիվանագիտության վրա ՏՀՏ-համացանցի ազդեցության և ՏՀՏ-համացանցի կառավարման վերաբերյալ: Նա դասավանդել է Մալթայի դիվանագիտական հետազոտությունների միջերկրածովյան ակադեմիայում, Նիդեռլանդիայի միջազգային հարաբերությունների ինստիտուտում (Քլինգենդալ), Ժնևի միջազգային հետազոտությունների և զարգացման հիմնախնդիրների ինստիտուտում, ՄԱԿ-ի համակարգի անձնակազմի քոլեջում և Հարավային Կալիֆորնիայի համալսարանում:

Կուրբալիան մշակել և ներկայում ղեկավարում է DiploFoundation հիմնադրամի «Համացանցի կառավարման բնագավառում ներուժի զարգացման ծրագիրը» (2005–2009):

Յովան Կուրբալիայի հետաքրքրություն ներկայացնող հիմնական հետազոտություններն են՝ համացանցի միջազգային կարգի ձևավորումը, համացանցի կիրառումը դիվանագիտության մեջ և բանակցություններում, համացանցի ազդեցությունը ժամանակակից միջազգային հարաբերությունների վրա:

Նա բազմաթիվ գրքերի, հոդվածների և աշխատությունների առանձին գլուխների հեղինակ է և խմբագիր: Նրա աշխատություններից են՝ «Համացանցի ուղեցույց դիվանագետների համար», «Գիտելիք և դիվանագիտություն», «Տեղեկատվական տեխնոլոգիաների ազդեցությունը դիվանագիտության վրա», «Զարգացող երկրների տեղեկատվական տեխնոլոգիաները և դիվանագիտական ծառայությունները», «Արդի դիվանագիտությունը», «Լեզու և դիվանագիտություն»:

Ստեֆանո Բալդիի և Էդուարդո Գելբշթայնի հետ նա համահեղինակ է ութ բրոշյուրից բաղկացած «Տեղեկատվական հասարակության գրադարան» շարքի, որում քննարկվում է համացանցին առնչվող տարբեր հարցերի լայն շրջանակ:

jovank@diplomacy.edu

ՀԱՄԱՑԱՆՑԻ ԿԱՌԱՎԱՐՈՒՄ

Յովան Կուրբալիա

4-րդ հրատարակություն

Ձևավորումը՝	Զորան Մարչետիչ, Դիանա Գրիգորյան
Խմբագիր՝	Իգոր Մկրտումյան
Հրտ. խմբագիր՝	Հայկազ Բաղյան
Գիտ. խմբագիր՝	Նարինե Խաչատրյան
Թարգմանիչներ՝	Փառանձեմ Շահվերդյան, Անի Բաղյան

«Նոյյան Տապան» տպագրատուն
Թուղթ՝ օֆսեթ N1, 60x84 1/16 ծավալը՝ 4,875 տպ. մամուլ
ստորագրված է տպագրության 13/02/12, տպաքանակը՝ 500
ՀՀ, Երևան 0009, Իսահակյան 28, հեռ.՝ (+37410) 565965
E-mail: contact@nt.am
URL: http://www.nt.am

Հաճախակի օգտագործվող հապավումների ցանկ

APEC	Asia-Pacific Economic Co-operation
ccTLD	country code Top-Level Domain
CIDR	Classless Inter-Domain Routing
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DRM	Digital Rights Management
GAC	Governmental Advisory Committee
gTLD	generic Top-Level Domain
HTML	HyperText Markup Language
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
aICT	Information and Communications Technology
IDN	Internationalized Domain Name
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet Protocol
IPR	Intellectual Property Rights
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
IXP	Internet eXchange Point
MoU	Memorandum of Understanding
OECD	Organisation for Economic Co-operation and Development
PKI	Public Key Infrastructure
S&T	Science and Technology
SGML	Standard Generalized Markup Language
sTLD	sponsored Top-Level Domain
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLD	Top-Level Domain
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UDHR	Universal Declaration of Human Rights
UDRP	Uniform Domain-Name Dispute-Resolution Policy
UNECOSOC	United Nations Economic and Social Council
UNCITRAL	United Nations Commission on International Trade Law
UNESCO	United Nations Educational, Scientific and Cultural Organization
VoIP	Voice-over Internet Protocol
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society
XML	eXtensible Markup Language

Հայաստանում առաջին անգամ հրատարակվող այս գիրքը Համացանցի Կառավարման յուրահատուկ տեղեկատու է: DiploFoundation Հիմնադրամի տնօրեն Յովան Կուրբալիյայի գրքում ներկայացված են համացանցի կառավարման տեխնիկական, տնտեսական ու սոցիալ-մշակութային տեսակետներն ու զարգացման հեռանկարները:

Համացանցի արդյունավետ կառավարումը հնարավոր է միայն պետական կազմակերպությունների, բիզնես համայնքի և քաղաքացիական հասարակության ակտիվ և կառուցողական փոխգործակցության շնորհիվ: Եվ պատահական չէ, որ այս գրքի բովանդակության և մոտեցումների վրա հիմնված ուսումնական ծրագրով 1997 թ.-ից ի վեր Դիպլո Հիմնադրամում ավելի քան 1000 դիվանագետներ, պետական ծառայողներ, ոչ կառավարական կազմակերպությունների աշխատակիցներ և ՏՀՏ մասնագետներ են վերապատրաստվել:

DiPLO www.diplomacy.edu
Internet Society Armenia Chapter
MEDIA EDUCATION