ՀԱՄԱՑԱՆՑԻ ԿԱՌԱՎԱՐՈՒՄ

Յովան Կուրբալիա

5-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: Ի՞նչ 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 հրատարակվող 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:

ՀԱՄԱՑԱՆՑԻԿԱՌԱՎԱՐՈՒՄ / Յովան Կուրբալիա- Երևան, Նոյյան Տապան, 2012, 246 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

ՀԿISBN: 978-99932-53-23-5

Բովանդակություն

Առաջաբան

Երբ 2004թ. ընկերներիս պատմեցի, թե ինչով եմ զբաղվում որպես WGIG-ի՝ Համացանցի կառավարման աշխատանքային խումբի անդամ, նրանք հաճախ էին ինձ դիմում տպիչների վերանորոգման կամ նոր ծրագրաշարերի տեղադրման խնդրանքով:
Նրանք կարծում էին՝ ես զբաղված եմ համակարգիչներին վերաբերող ինչ-որ գործով: 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 այն պատճառներից մեկը՝ ինչու առաջացավ Դիպլո-ի դասագրքի և համացանցի կառավարման նկարների ստեղծման մտահղացումը:
Այսօր՝ ընդամենն ութ տարի անց, նույն մարդիկ, ովքեր նախկինում խնդրում էին համակարգիչը կարգաբերել, արդեն հարցնում ինձ, թե ինչպես պաշտպանել իրենց մասնավոր կյանքը ֆեյսբուքում կամ ինչպես ապահովել իրենց երեխաների ապահով և անվտանգ աշխատանքը Համացանցում: Ավելին, նրանք մտահոգված են հնարավոր կիբեռպատերազմով և ջրամատակարարման, էլեկտրակայանների և իրենց քաղաքում կամ երկրում առկա այլ կաևոր ինֆրաստուրկտուրաների հետ առնչվող առցանց ռիսկերով: Ինչպիսի՞ առաջընթաց ենք մենք ապրել:
Համացանցի կառավարումը ավելի ու ավելի հանրային է դառնում: Որքան Ժամանակակից հասարակությունը կախված է Համացանցից, այնքան պահանջված է դառնում Համացանցի կառավարումը: Համացանցի կառավարումը վերաբերում է բոլորիս, անկախ նրանից՝ մենք վերջինիս երկու միլիարդ օգտատերերից ենք, թե՝ ոչ, քանի որ չօգտվողները նույնպես կախված են Համացանցի ծառայություններից:
Համացանցի կառավարումն առավել կարևոր է նրանց համար, ովքեր խորապես ինտեգրված են էլեկտրոնային աշխարհում՝ էլեկտրոնային բիզնեսի կամ պարզապես ֆեյսբուքի միջոցով: Այնուամենայնիվ, այն վերաբերում է նաև պետական պաշտոնյաներին, զինծառայողներին,

իրավաբաններին, դիվանագետներին՝ բոլոր նրանց, ովքեր հանրային շահն են պաշտպանում կամ էլ հանրային կայունությունը: Մասնավորապես, պաշտպանում է մասնավոր կյանքի գաղտնիությունը, մարդու իրավունքները և գտնվում է քաղաքացիական հասարակության, ոչ-կառավարական կազմակերպությունների կիզակետում: Վաղվա Google, Skype, Facebook, և Twitter ստեղծողները նավարկում են ցանցում արդեն այսօր: Նրանց ստեղծագործությունը և նորարարությունը չպետք է խոչընդոտել, այլ խրախուսել Համացանցի զարգացման նոր ավելի ստեղծագործ ուղիներ գտնելու համար: Համացանցի կառավարման հիմնական նպատակներից մեկը, զարգացման համար անհրաժեշտ և այնպիսի բարենպաստ իրավաքաղաքական 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 ծանոթանում այս առարկային: Մյուսների համար գիրքը պարզապես կօգնի վերհիշել այն ամենը, ինչ նրանք արդեն անում են իրենց մասնագիտական բնագավառում, լինի դա e-առողջապահություն, e-առևտուր, e-կառավարում, e-ցանկացած բնագավառ, որը Համացանցի կառավարման խնդիրների մաս է կազմում:
Այս տարաբնույթ մոտեցման հիմքում ընկած է մի ցանկություն. աշխարհի միլիարդավոր մարդկանց համար Համացանցը ինտեգրված և բարենպաստ միջավայր պահպանելու գործում իմ համեստ ներդրումն ունենալ: 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/ հասցեով:

Յովան Կուրբալիա
DiploFoundation
Հոկտեմբեր 2012թ.

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

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:

Ինչ էնշանակում «համացանցի կառավարում» տերմինը

Տեղեկատվական հասարակության հարցերով համաշխարհային

գագաթնաժողովի (WSIS)1 շրջանակներում առաջարկվել է համացանցի կառավարման հետևյալ սահմանումը. «Համացանցի կառավարումը համացանցի զարգացումն ու օգտագործումը կանոնակարգող կառավարությունների, մասնավոր սեկտորի և քաղաքացիական հասարակության կողմից համապատասխան ընդհանուր սկզբունքների, նորմերի, կանոնների, ընդունված 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:

«Համացանց» կամ «համացանց» և քաղաքական ազդակները

2003թ.-ին The Economist ամսագիրը սկսեց համացանց բառը գրել փոքրատառ “i” տառով: Խմբագրության քաղաքականության մեջ այս փոփոխությունը ոգեշնչված էր այն փաստով, որ Համացանցը դարձել էր առօրեական, այլևս ոչ եզակի կամ ոչ բավարար առանձնահատուկ նախնական կապիտալ: «Համացանց» բառը կրկնեց հեռագրության, հեռախոսի, ռադիոյի, հեռուստատեսության և այլ նմանատիպ հայտնագործությունների լեզվաբանական ճակատագիրը: «Համացանց» բառը մեծատառով կամ փոքրատառով գրելու հարցը կրկին բարձրացվեց 2006թ.-ի նոյեմբերին Անթալիայում Հեռահաղորդակցության միջազգային միավորման (ITU) համաժողովի շրջանակներում, որտեղ քաղաքական տարաձայնություններ առաջացան, երբ Համացանցի կառավարման վերաբերյալ ITU-ի որոշման մեջ «Համացանց» տերմինը հանդես եկավ փոքրատառով: ԱՄՆ-ի դեսպան՝ Դեյվիդ Գռոսը ի լրումն Համացանցի կառավարման, իր մտահոգությունը հայտնեց նաև այն հարցի շուրջ, որ ITU-ի փոքրատառ ուղղագրությունը կարող է Համացանցին այլ հեռահաղորդակցական համակարգերի պես վարվելու ազդակ ծառայել: Ոմանք մեկնաբանեցին, որ սա ITU -ի՝ Համացանցի կառավարման հարցում առավել նշանակալից դեր խաղալու մտադրության քաղաքական ազդակ է:

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 (gestão publica, administracăo 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 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]

Նախածանցներ. e-/ վիրտուալ / կիբեռ/ թվային

e- /վիրտուալ / կիբեռ / թվային նախածանցները սովորաբար օգտագործվում են տարբեր ՏՀՏ/ Համացանցային զարգացումներ նկարագրելու համար: Վերջիններիս օգտագործումը սկսվեց 1990-ականներին և ենթադրում է տարբեր հասարակակն, տնտեսական և քաղաքական ազդեցություններ Համացանցի զարգացման հարցում: Օրինակ՝ e- նախածանցը սովորաբար ասոցացվում է էլեկտրոնային առևտրի (e-commerce) և 1990-ականների վերջում Համացանցի՝ առևտրի ոլորտ մտնելու հետ: Գիտնականները և Համացանցի պիոներներն օգտագործում էին և՛ կիբեռը, և՛ վիրտուալը Համացանցի նորությունը և նոր, համարձակի աշխարհի առաջացումն ընդգծելու համար: Թվային տերմինը հիմնականում սկսեց օգտագործվել տեխնիկական բնագավառում և ճանաչում գտավ թվային բաժանման քննարկման շրջանակներում:
Միջազգային ասպարեզում կիբեռ նախածանցն օգտագործվեց Եվրոխորհրդի կողմից 2001թ.-ին Կիբեռհանցագործության բնորոշման համար: Վերջերս այն օգտագործվել էր կիբեռանվտանգության հարցերի շրջանակներում: ITU-ն իր նախաձեռնություններն այս բնագավառում անվանեց Գլոբալ կիբեռանվտանգության օրակարգ: Վիրտուալ բառը հազվադեպ է հայտնվում միջազգային փաստաթղթերում: e- նախածանցը ԵՄ-ում հատուկ նշանակություն ունի, որտեղ այն նկարագրում է էլեկտրոնային գիտության (e-science) և բժշկության (e-health) տարբեր քաղաքականություններ: WISIS-ի գործընթացի ընթացքում e- նախածանցը ներմուծվեց Համաեվրոպական Բուխարեստյան տարածաշրջանային հանդիպման շրջանակներում և դարձավ գերակշռող WSIS-ի բոլոր տեքստերում՝ ներառյալ վերջնական փաստաթղթերում: WSIS-ի գործունեությունը կենտրոնացված է գործնական ոլորտներում՝ ներառյալ էլեկտրոնային կառավարություն(e-government), բիզնես (e-business), կրթություն (e-learning), առողջապահություն (e-health), զբաղվածություն (e-employment), գյուղատնտեսություն (e-agriculture), գիտություն (e-science):

«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 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 ստեղծվեց 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 գագաթնաժողով (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 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.-ի զարգացումները

2005 թ. նոյեմբերին Թունիսում տեղի ունեցած հանդիպման ավարտից հետո 2006 թ. համացանցի կառավարման հարցերով բանավեճերի առարկա դարձան երեք կարևորագույն իրադարձություններ: 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

միջազգայնացման 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) լիագոր 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 նկատմամբ:

2007թ.-ի զարգացումները

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՝ արդյոք ICANN-ն 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.-ի զարգացումները

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 միջազգայնացման 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 Face-

book –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: Տարբեր պատճառներով, բիզնեսի այս բնագավառի ներկայացուցիչները նախընտրում են ցանցով հաղորդվող տվյալների առնչությամբ որոշակի տարբերակում: 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.-ի զարգացումները

2009 թ.-ի 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 «բաց համացանցի» սկզբունքների հանդեպ: Նախընտրական քարոզարշավի ընթացքում տված խոստումների համաձայն՝ նրա թիմը ցանցային չեզոքության սկզբունքին աջակցելու մի շարք միջոցառումներ իրականացրեց: 2009 թ.-ի 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.-ի 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.-ի զարգացումները

2010թ.-ի օգոստոսի դրությամբ համացանցի կառավարման ոլորտի ամենաառաջնահերթ զարգացումները վերաբերել են Facebook-ի, Twitter-ի և նմանատիպ սոցիալական պլատֆորմների ազդեցության աճին: Կարևորագույն խնդիրներից մեկը օգտվողների անձնական կյանքին վերաբերող գաղտնիության 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 մնալ 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:

2011թ.-ի զարգացումները

2011թ.-ի կարևորագույն զարգացումը եղավ Համացանցի կառավարումը գլոբալ քաղաքականության առավել բարձր օրակարգում բարձրացնելը: Համացանցի կառավարման ակտուալությունը մոտեցավ այնպիսի քաղաքական հարցերին, ինչպիսիք են կլիմայական փոփոխությունները, միգրացիան և սննդի անվտանգությունը: Համացանցի քաղաքական ակտուալության մյուս հետևանքը եղավ Համացանցի կառավարման աստիճանական տեղաշարժը տեխնիկական ազգային ծածկույթից (IT, հեռահաղորդակցություն) դեպի քաղաքական կառույցներ (դիվանագիտություն, վարչապետական նստավայր): Ի լրումն այս ամենի՝ հիմնական միջազգային ԶԼՄ-ները (օրինակ՝ The Economist, IHT, Al Jazeera, BBC) ևս սկսեցին առավել մանրամասն, քան երբևէ հետևել

Համացանցի կառավարման զարգացումներին:Համացանցի կառավարման վրա ազդեցություն ունեցավ նաև «Արաբական գարունը»: Չնայած որ չա-փազանց տարբեր տեսակետներ կային կապված Համացանցի ազդեցության հետ «Արաբական գար-նան» ֆենոմենի վրա, այնուամենայնիվ մեկ եզրակացույուն հստակ է. Սոցիալական լրատվամիջոցներն ընկալվում են որպես որոշիչ գործիքամիջոցներ ժամանակակից քաղքական կյանքում: Տարբեր եղանակ-ներով Համացանցը և նրա կառավարումը այս տարվա ընթացքում բարձրացան ողջ աշխարհի քաղա-քական դիտակետում: Հունվարի 27-ին եգիպտական իշխանություններն անջատեցին Համցանցին հասանելիությունը՝ քաղա-քական բողոքները դադարեցնելու իզուր հույսեր ունենալով: Սա եղավ կառավարության հանձնարա-րությամբ մի ողջ երկրում համացանցի ամբողջական դադարեցման առաջին օրինակը: Նախկինում՝ նույ-նիսկ ռազմական հակամարտությունների (նախկին Հարավսլավիա, Իրաք) ժամանակ դեռ երբեք Համացանցով հաղորդակցությունն ամբողջությամբ չէր դադարեցվել:Հիլարի Քլինտոնի Համացանցում ազատ արտահայտման նախաձեռնությունը, որը սկսվել էր 2010թ.-ի փետրվարի նրա ելույթով, արագացվեց 2011թ.-ին:
Այս թեմայով երկու հիմնական համագումար կա-յացավ. Մարդու իրավունքների և Համցանցի վերաբերյալ Վիեննայի համաժողովը, Համացանցի և ազա-տության վերաբերյալ Հաագայի համաժողով:
2011թ.-ին ICANN-ը շարունակեց իր էության հիմնական զարգացումները հետևյալ ուղղություններով.

- կառավարման կիրառման բարեփոխումներ,
- նոր, բարձր մակարդակի դոմեյնների(gTLDs) ներմուծման վերջնական քաղաքականության պատրաստում,
- վերջինիս գլխավոր գործադիր տնօրենի գրանցում և փոխարինման համար փնտրում:

2011թ.-ը բնորոշվեց նաև Համացանցի կառավարման սկզբունքների հոսքով, որոնք առաջարկել էին OECD-ն, Եվրոխորհուրդը, ԵՄ-ը, Բրազիլիան և այլ մասնակիցներ: Այս սկզբունքների բազմաթիվ համակ-ցությունները կարող էին ապագայում Համացանցի վերաբերյալ նախնական գլոբալ դեկլարացիայի կամ նմանատիպ փաստաթուղթի նախաբանը դառնալ, որը կարող էր որպես հիմք ծառայել Համացանցի կառավարման զարգացման համար:

Համացանցի կառավարման վերլուծական գործիքներ

Լիակատար ճշմարտությունը բացահայտվում է այն փաստով, որ վերջինիս հակառակը նույնպես լիակատար ճշմարտություն է՝ ի հակադրություն սովորական ճշմարտության, որի հակառակը ակնհայտ անհեթեթություն է:
Նիլս Բոռ, ականավոր ֆիզիկոս(1885-1962)

Համացանցի կառավարման վերլուծության գործիքները քաղաքական փաստարկներ նախապատրաստելու և քաղաքական ուղղություն մշակելու համար նախատեսված գործիքների հավաքածու է: 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» և «սահմանափակ» մոտեցում

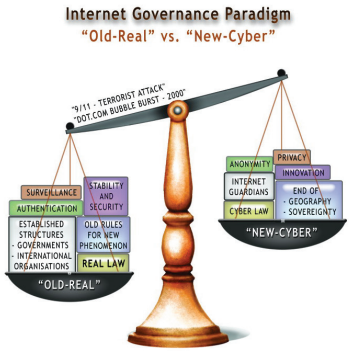
«Սահմանափակ» մոտեցման դեպքում ուշադրությունն, առաջին հերթին, կենտրոնացած է լինում համացանցի ենթակառուցվածքի վրա (դոմենային անունների, IP հասցեների և «արմատական» սերվերների համակարգերի) և ICANN դիրքերի վրա՝ որպես այդ դաշտի գլխավոր խաղացողի:
«Ընդարձակ» մոտեցման համաձայն, համացանցի կառավարման վերաբերյալ բանակցությունները պետք է դուրս գան ենթակառուցվածքի հարցերի սահմաններից ու դիմեն այլ՝ իրավական, տնտե-սական, սոցմշակութային, զարգացման հետ կապված հարցերի: Այս վերջին մոտեցումը հաստատված է WGIG հաշվետվությունում և WSIS ամփոփոխ փաստաթղթում: Այն ընկած է նաև IGF ճարտարապե-տության սկզբունքների հիմքում:

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 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» մոտեցումն ընդդեմ «նոր կիբեռմոտեցման»



Համացանցի կառավարման շրջանակում յուրաքանչյուր հարց կարելի է դիտարկել երկու տարբեր կողմերից: «Հին իրական» մոտեցման համաձայն՝ համացանցը կառավարման բնագավառում ոչ մի նոր բան չի ներմուծել: Համացանցը ևս մեկ տեխնիկական միջոց 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 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 կառուցվածքն ընդդեմ կենտրոնացված կառուցվածքի

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 որ 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

Համացանի տեխնոլոգիան շատ արագ է զարգանում: Նոր ծառայությունները ներմուծվում են գրեթե յու-րաքանչյուր օր: Այս ամենը ստեղծում է լրացուցիչ դժվարություններ Համացանցի կառավարման բնագա-վառում: Օրինակ՝ 2005թ.-ի նոյեմբերին, երբ Համացնցի կառավարման վերաբերյալ բանակցություններն ընթանում էին Թունիսում՝ WSIS-ի շրջանակներում, Twitter-ը գոյություն չուներ: Այժմ Twitter-ը բարձրաց-նում է Համացանցի կառավարման հիմանակն հարցերից մեկը, ինչպիսին է անձնական կյանքի գաղտ-նիությունը, արտահատման ազատությունը և մտավր սեփականության պաշտպանությունը: Տեխնոլոգիայի արագ փոփոխման մեկ այլ օրինակ է սփամի արդիականությունը: Դեռ վաղ 2005թ.-ին այն կառավարման հիմնական հարցերից էր: Այժմ բարդ բարձր տեխնոլոգիական ֆիլտրների շնորհիվ սփամը հազվադեպ է քննարկվում Համացանցի կառավարման ժողովների ժամանակ:

Քաղաքական հավասարակշռության գործառույթներ

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՝

- արտահայտման ազատության և հասարակական կարգի պահպանման միջև հակասությունը: Համացանցում իր արտացոլումն է գտել Մարդու իրավունքների համընդհանուր հռչակագրի 19 (ինքնարտահայտման ազատություն) և 27 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:

Շատերը քննադատում են այս «հավասարակշռության զույգերը»՝ դրանք համարելով սխալ երկիմաստութ-յուններ: Օրինակ՝ կան ուժեղ փաստարկներ, որ կիբեռանվտանգությունը պարտադիր կերպով չի նշանա-կում ավելի քիչ մասնավոր կյանքի գաղտնիություն: Կան մոտեցումներ, որոնք ուժեղացնում են թե՛ կիբեռ-անվտանգությունը, թե՛ մասնավոր կյանքի գաղտնիությունը: Մինչ այս երկու տեսակետները ուժեղորեն պահպանվում են, Համացանցի կառավարման քաղաքականության իրականությունը ենթադրում է վերը նշված մոտեցման երկակիությունը:

Քաղաքականության հավասարակշռման գործողություններ պատմության մեջ

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:

«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 դրոշմանիշերի պահպանումը, էլեկտրոնային առևտրի հարկադրում),
- համացանցում կիրառելիներն՝ առանց էական փոփոխությունների (օրինակ՝ խոսքի ազատության պաշտպանությունը):

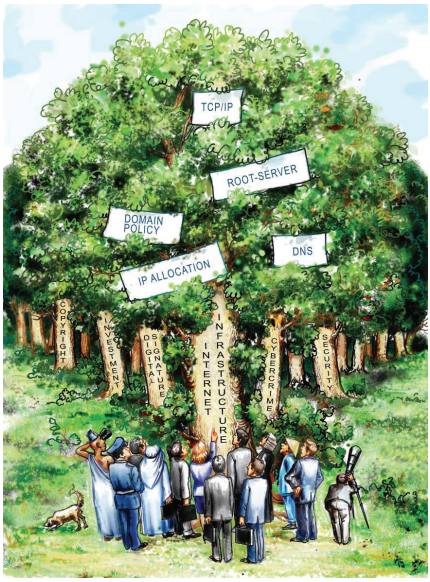
Գոյություն ունեցող նորմերի կիրառումը կարող է նկատելիորեն բարձրացնել իրավական կայունությունն ու հեշտացնել համացանցի կառավարման կարգ ստեղծելու խնդիրը:

«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):

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 չեզոքության սկզբունքի օգտագործումը ստեղծում է մի քանի մասնավոր և տվյալների պաշտպանության միջոցներ, որոնցից է նույնքան արդիական Տնտեսական համագործակցության և զարգացման կազմակերպությունը (OECD)՝ ստեղծված 1980թ.-ին:
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:

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:

Խուսափեք ծրագրային կոդի օգնությամբ հասարակությանը կառավարելու ռիսկից

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 մնում 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 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

Նոր բարդ համանմանություն ստեղծվել էր VoIP-ի (օր.՝

Skype) կողմից, որն իրենից ներկայացնում է հեռա-խոսի ֆունկցիոնալություն Համացանցի արձանագրություններն (protocol) օգտագործելով: Այս հաջորդա-կանությունն առաջացրեց քաղաքականության հակասություններ Դուբայում Աշխարհի միջազգային հեռահաղորդակցույան համաժողովի (WCIT) պատրաստությունների ընթացքում: Ընթացիկ կարծիքը, թե VoIP-ն հանդիսանում է Համացանցի ծառայություն վիճարկվում է այն մարդկանց կողմից, ովքեր կարծում են՝ վերջինս, ինչպես հեռախոսակապը, պետք է կարգավորվի ITU-ի կողմից գլոբալ մակարդակի վրա:

Փոստային ծառայությունը և ICANN-ը

Պոլ Թվոմին՝ ICANN-ի նախկին գործադիր տնօրենը, օգտագործում էր փոստային համակարգի և ICANN-ի միջև հետևյալ համանմանությունը. եթե Դուք Համացանցը դիտարկում եք որպես փոստային բաժանմունք կամ փոստային համակարգ, ապա դոմենը և IP հասցեն հիմնովին երաշխավորում են, որ ծրարի վրա գրված հասցեներն աշխատում են: Դրանք նախատեսված չեն իմանալու համար, թե ինչ կա ծրարի ներսում, ով է ուղարկել ծրարը, ում է թույլատված կարդալ ծրարը, ինչքան ժամանակ է տևում ծրարը տեղ հասցնելու համար, ինչ արժե ծրարը: Նշված հարցերից և ոչ մեկը կարևոր չէ ICANN-ի գործունեության համար: Նրա ֆունկցիան կայանում է միայն հասցեների աշխատանքն ապահովելու մեջ:

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 հիմնախնդիրը 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 պոռնոգրաֆիական 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:

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 կարո՞ղ 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:

Համացանցը և մայրուղիները

ITU-ի գլխավոր քարտուղար Համադուն Թուռն օգտագործում է Համացանցի և մայրուղիների միջև համանմանությունը՝ մայրուղիները հեռահաղորդակցությանը նմանեցնելով, իսկ Համացանցը երթևեկության մեքենաներին.«Ես մի օրինակ եմ բերում՝ համեմատելով Համացանցը և հեռահաղորդակցությունը մեքենաների և մայրուղու հետ: Եթե մայրուղին Ձեզ է պատկանում, ապա դա չի նշանակում, որ նրանով ընթացող մեքենաները ևս Ձեզ են պատկանում, առավել ևս նրանցում գտնվող իրերը, և հակառակը: Սա պարզ համանմանություն է: Բայց Ձեր երթևեկությունը սահուն տանելու համար Դուք պետք է իմանաք, երբ եք կառուցում Ձեր ճանապարհները, մեքենաների լայնությունը, բարձրությունը և արագությունը, որպեսզի կամուրջները համապատասխան կերպով կառուցեք: Հակառակ դեպքում համակարգի չի աշխատի: Ինձ համար սա է նմանությունը Համացանցի և հեռահաղորդկացության մեջ: Նրանք դատապարտված են միասին աշխատելու» :

Համացանց-մայրուղի

Ընդհանուր գծեր

Այն, ինչ մայրուղին իրական կյանքում հանդիսանում է երթևեկության մեջ, Համցանցը հանդիսանում է կապի համար վիրտուալ տարածությունում:

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 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:

Տարբերությունները

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:
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:

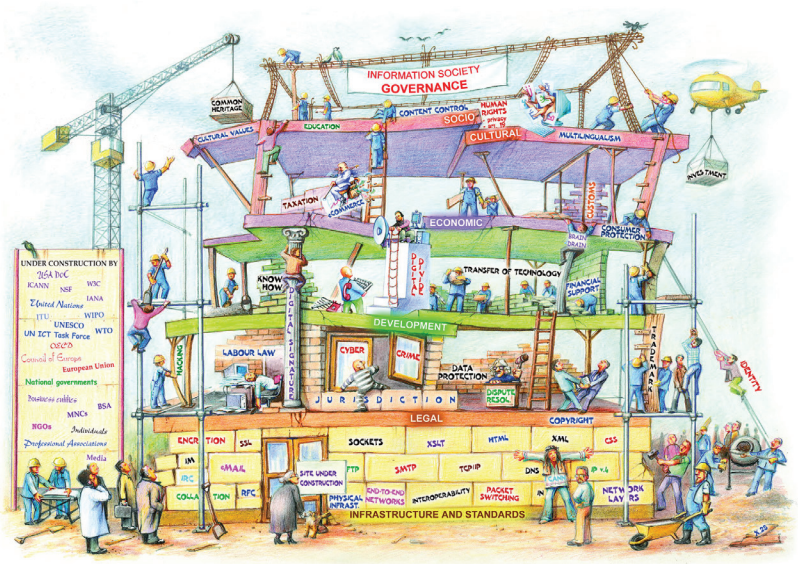
2006 թ. Աթենքում տեղի ունեցած Համացանցի կառավարման առաջին համաժողովի օրակարգում ընդգրկված էր հետևյալ լուծում պահանջող ոլորտների քննարկումը՝

- 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 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 հետևյալ հինգ զանբյուղների.

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

Diplo-ի մշակած դասակարգումն արտացոլում է, ինչպես վերը հիշատակված WGIG և IGF քաղաքական մոտեցումները, այնպես էլ տվյալ ոլորտում գիտական հետազոտությունների արդյունքները: Դասակարգումը ստեղծվել է 1997թ.-ին հաստատուն կարգավորմամբ՝ հիմնվելով ուսանողների (2011թ.-ի շրջանավատներից 1015 ուսանող) արձագանքների, հետազոտությունների արդյունքների և քաղաքական գործընթացի գաղափարների վրա:

Ծանոթագրություն.

1The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis, from 16 to 18 November 2005. The objective of the first phase was to develop and foster a clear statement of political will and to take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake. More than 19 000 participants from 174 countries attended the summit and related events. Source: http://www.itu.int/wsis/basic/about.html [accessed 16 October 2012].

2 The WGIG definition follows the pattern of frequently used definitions in the regime theory. The founder of regime theory, Stephen D. Krasner, notes that: Regimes can be defined as sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behaviour de„ ned in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice. Krasner S (1983) Introduction, in International Regimes. Krasner SD (ed.), Cornell University Press: Ithaca, NY, USA.

3 Shannon V (2006) What's in an 'i'? International Herald Tribune, 3 December 2006. Available at: http://www.nytimes.com/2006/12/03/technology/03iht-btitu.3755510. html?pagewanted=all&_r=0 [accessed 16 October 2012].

4 The technological confusion was highlighted by the way the term 'governance' was used by some international organisations. For example, the term 'good governance' has been used by the World Bank to promote the reform of states by introducing more transparency, reducing corruption, and increasing the efficiency of administration. In this context, the term 'governance' is directly related to core government functions.

5 Barlow JP (1996) A declaration of the independence of cyberspace. Available at: https://projects.eff.org/~barlow/Declaration-Final.html [accessed 16 October 2012].

6 For the evolution of the use of the word 'Internet' in the preparation for the Geneva summit: DiploFoundation (2003) The Emerging Language of ICT Diplomacy – Key Words. Available at: http://archive1.diplomacy.edu/IS/Language/html/words.htm [accessed 16 October 2012].

7 In June 2010, ICANN approved the .XXX top level domain name for adult material.

8 Network neutrality is a principle proposed for user access networks participating in the Internet that advocates no restrictions by Internet Service Providers and governments on content, sites, platforms, on the kinds of equipment that may be attached, and no restrictions on the modes

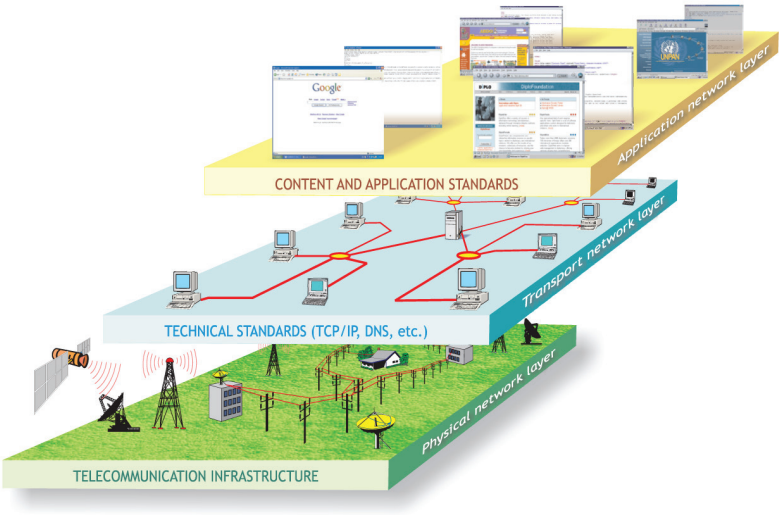
of communication allowed. The principle states that if a given user pays for a certain level of Internet access, and another user pays for the same level of access, then the two users should be able to connect to each other at the subscribed level of access. (Source: Wikipedia).
9 Available at: http://www.state.gov/secretary/rm/2010/01/135519.htm [accessed 16 October 2012].
10 This section could not have been completed without discussion with Aldo Matteucci, Diplo's senior fellow, whose 'contrarian' views on modern governance issues are a constant reality check in Diplo's teaching and research activities.
11 Barlow (1996) op. cit.
12 The WSIS process started with the first preparatory meeting held in July 2002 in Geneva. The first summit was held in Geneva (December, 2003) and the second summit in Tunisia (November, 2005).
13 Volker Kitz provides an argument for the analogy between administration of telephony systems and Internet names and numbers. Kitz V (2004) ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called 'uniqueness' of the Internet. Available at: http://studentorgs.law.smu.edu/Science-and-Technology-Law- Review/Articles/Fall-2005/Kitz.aspx [accessed 16 October 2012].
14 Excerpts from the Secretary General's speech delivered at the ICANN meeting in Cairo (6 November 2008). Available at: https://cai.icann.org/files/meetings/cairo2008/toure-speech-06nov08.txt [accessed 16 October 2012].
15 Quoted in Mock K, Armony L (1998) Hate on the Internet. Available at http://www. bnaibrith.ca/league/hoti/hoti-00.html [accessed 20 October 2012].
16 The term 'basket' was introduced into diplomatic practice during the Organization on Security and Cooperation in Europe (OSCE) negotiations.

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 վիճակը

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, 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:

ITU-ի Միջազգային հեռահաղորդակցման կարգավորումը (ITR)

1988թ.-ին ITU-ի Միջազգային հեռահաղորդակցման կարգավորումը (ITR) նպաստեց գների և ծառայությունների ազատականացմանը և թույլատրեց Համացանցի հիմնական ծառայությունների առավել նորարական օգտագործումը, ինչպիսիք են միջազգային տրամադրված գծերը: Դա 1990-ականներին Համացանցի դանդաղ զարգացման կառուցողական հիմք ստեղծեց:

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:

Հեռահաղորդակցության 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]: Այս հարցը կրկին ի հայտ եկավ 2012.-ի Միջազգային հեռահաղորդակցության վերաբերյալ աշխարհի համաժողովի (WCIT-2012) շրջանակներում, երբ որոշ զագացող երկրներ բարձրացրեցին Համացանցի ծառայություններից ստացվող եկաումտների վերաբաշխման հարցը (հավելյալ տեղեկատվության համար կարող եք տե՛ս Զարգացման զամբյուղը):

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:

Ում է պատկանում էլեկտրամագնիսական սպեկտորը

Սկեկտրի կառավարման ներկա ընթացակարգը հիմնված է այն ենթադրության վրա, որ վերջինս հազվա-գյոտ ռեսուրս է, որը պետք է ղեկավարվի կառավարական ինստիտուտների, ռեգիոնալ մարմինների (ինչ-պիսին է ԵՄ-ն Ռադիոյի սպեկտրի կոմիտեն (RSP) և Ռադիոյի սպեկտրի քաղքականության խումբը(RSPG)) և ITU-ի կողմից: Այս բնագավառում վերջին հետազոտությունը հաստատեց, որ այս սպեկտրը սահմանափակ ռեսուրս չէ: Հակառակը, սպեկտրի օգտագործման ծավալը և

սահմանափա-կումները կախված են սարքի՝ էլեկտրոնային ազդանշաններ ուղարկելու և ստանալու ունակությունից:
Այս մոտեցումը վիճարկում էր, որ ներկա կառավարական կարգավորումը պետք է փոխարինվի «բաց սպեկտրով», այսինքն՝ բոլորի համար բաց հասանելիությամբ:
Այս տեսակետի հետ կապված երկու պոտենցիալ խնդիրներ կան: Մեկը գործնական է և կապված է այն հսկայական ներդրումների հետ, որոնք հեռահաղորդակցության կազմակերպությունները, մասնավորապես Եվրոպայում, կատարել են երրորդ սերնդի բջջային հեռախոսների ցանցերի օգտագործ-ման իրավունք ձեռք բերելու համար: Մյուս խնդիրը կայանում է նրանում, որ եթե սպեկտրը դառնա բոլորի համար ազատ, ապա դա պարտադիր կերպով չի նշանակում, թե ավտոմատ կերպով կդառնա հանրային բարիք: Ավելին, վերջինս կօգտագործվի նրանց կողմից, որքեր ունեն բավականաչափ բարդ սարքավորումներ. առավել հավանական է մեծ, մասնավոր կազմակերպությունների կողմից:
Ռադիոյի սպեկտրն օգտագործող նոր հեռահաղորդակցության զարգացումը, հատկապես անլար լայնա-շերտ և բջջային հեռահաղորդակցությունը, բարձրացրել են ռադիոհաճախականության պահանջարկը՝ կոչ անելով աշխարհի կառավարություններին սպեկտրի կիրառման օպտիմալ լուծում կիրառել: Լայնա-շերտ հեռուստատեսությունը թվայինով փոխարինելը թույլ կտա ազատականացնել ռադիոսպեկտրի կարևոր մասերից մեկը, որն այդպիսով կարող է հատկացվել այլ ծառայությունների, այսպես կոչված թվային դիվիդենտի: ԵՄ-ն մշակել է ռադիոսպեկտրի կառավարման բազմակողմանի կարգավորման ծրագիր, մինչդեռ ԱՄՆ-ն, հաճախականություններն վաճառքի գործընթացում առաջարեկելով, շուկայի առաջատարն է:

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

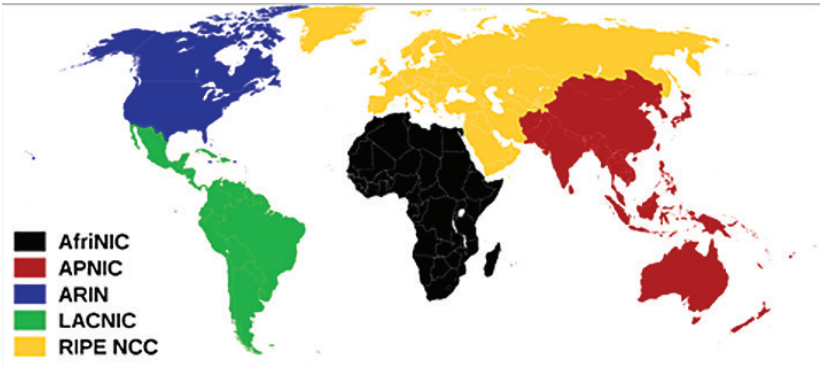
Արդի վիճակը

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 (RIR):



Տարածաշրջանային համացանցային մատենավարություններն, իրենց հերթին, հասցեները բաժանում են ազգային(NIR) ու տեղական համացանցային (LIR) մատենավարությունների միջև , իսկ դրանք IP հասցեները փոխանցում են ավելի ցածր աստիճանի, համացանցային ոչ մեծ ծառայություններ մատուցողներին, ընկերություններին և մասնավոր անձանց:

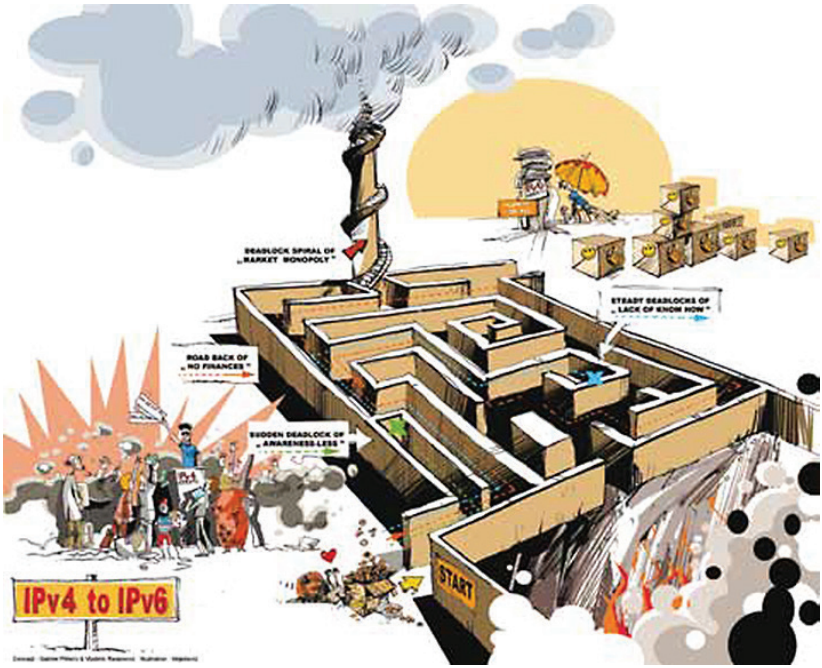
Հարցեր

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, որոնք 2011թ.-ի փետրվարին IANA կողմից ամբողջովին բաշխվել են հինգ RIR-երի միջև: 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 (340 000 000 000 000 000 000 000):

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:

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: 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 սկզբանե IPv6-ի վրա հիմնված ցանցեր ներմուծելու հնարավորությունից: Ներդրման ընթացքում զարգացող երկրներին տեխնիկական օգնություն ցուցաբերելու անհրաժեշտություն է լինելու8: 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 վերափոխում9:

Տեխնոլոգիան, ստանդարտները և քաղաքականությունը

Ցանցային արձանագրությունների շուրջ բանավեճերը ցույց տվեցին, թե ինչպես ստանդարտները կարող են քաղաքականացվել այլ նկատառումներից ելնելով: Մինչդեռ կառավարության միջամտությունը բիզնեսի և տեխնոլոգիայի բնագավառ (ինչպիսիք են ապահովության կարգավորումներ և հակամենաշնորհային գործառույթները) ակնհայտ է քաղաքական և հասարակական կարևորության պատճառով, ապա տեխնիկական ստանդարտները սովորաբար ենթադրում են սոցիալական չեզոքություն և, հետևաբար, քիչ պատմական հետքրքրություն ունեն: Սակայն տեխնիկական որոշումները կարող են հեռուն գնացող տնտեսական և սոցիալական հետևանքներ ունենալ՝ փոխելով հավասարակշռությունը մրցակցող ազգերի և ձեռնարկությունների միջև, հակադրելով օգտագործողների ազատությունը: Ձևական ստանդարտներ ստեղծելու ջանքերը բերում են համակարգի կառուցողների կողմից ստեղծված մասնավոր տեխնիկական որոշումների, որոնք կարող են առաջացնել անասելի ենթադրություններ և շահերի բախում: Այն բուռն վերաբերմունքը, որը ցուցաբերում են շահառուները ստանդարտները վիճարկելու հարցում, պետք է նախազգուշացնի մեզ «ընկույզի և հողյուսի» առավել խոր նշանակության մասին:

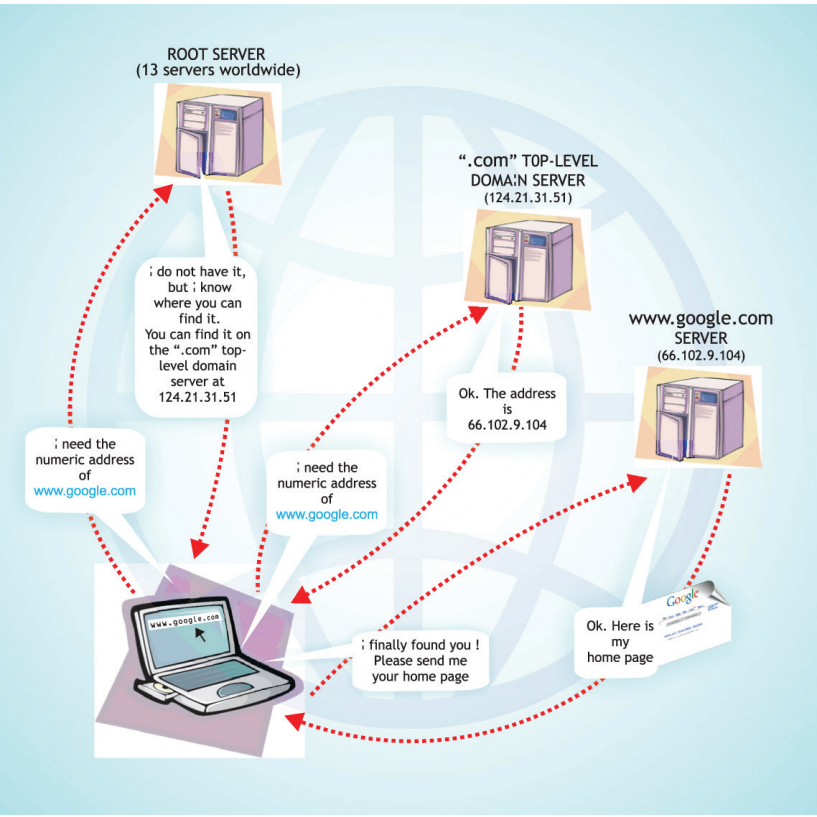
TCP/IP փոփոխությունը և անցագրային սահմանափակ ունակության հիմնախնդիրը

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 «Any-cast» 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 (cyber-squatting), 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: Այնուամենայնիվ, նոր gTLD-ների ներմուծը չափազանց դանդաղ ևվճարկելի գործընթաց էր: Նոր քաղաքականության՝ վեց տարի զարգացման և խորհրդակցության ընթացքում, ICANN-ը սկսեց նոր gTLD-ի կիրառումն այս տարի՝ 2012թ.-ին: Նոր ծրագրի շրջանակներում ցանկացած կազմակերպություն կարող է դիմել նոր gTLD ռեգիստր կիրառելու համար, ներառյալ ոչ լատինատառ լեզուների սկրիպտները: 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: Չնայած նոր gTLD-ի ներկայացման ժամանակառկա վեճերին՝ ծրագիրը գործարկվել է և աշխատում է. շուտով Համացանցի անունների տիրույթը ավելի մեծ կլինի:

ICANN-ը քննելով գործադրվող ճնշումները՝ վերին մակարդակի դոմենային նոր անունների ստեղծման հարցում, խորհրդատվությունների գործընթաց սկսեց, որն ուղղված էր այդ ոլորտում նոր քաղաքականության մշակմանը:

Մտավոր սեփականությունը միակ անհանգստությունը չէր

այս գործընթացում: Ամենից ուշագրավ իրավիճակը կապված էր մեծահասակների համար .xxx դոմեյնի ներմուծման առաջարկությունը: Առաջին անգամ 2000թ.-ին նախաձեռնած, ապա 2004թ.-ին վերաառաջարկված գաղափարը մերժվեց 2007թ.-ի մարտին ICANN-ի խորհրդի կողմից: Որոշման հիմնական քննադատության պատճառն այն էր, որ ICANN-ն այն ընդունել էր ԱՄՆ-ի կառավարության ճնշման ներքո, որն ուժեղորեն դեմ էր վերջինիս ներմուծ-մանը: ԱՄՆ կառավարության նման տեղաշարժը լայն արձագանքման արդյունք դարձավ: Դրանց թվում կային թերահավատ պնդումներ, որ .xxx դոմեյնը գրավիչ չի դառնա Համացանցի սեքս բիզնեսի համար, քանի որ խսորեն ֆիլտրման ռիսկ գոյություն ունի: 2010թ.-ի հունիսին հարցը վերանայվեց. ICANN-ի խորհուրդը դրական կերպով վերանայեց .xxx դոմեյնի կիրառումը, որը վերջապես հաստատվեց 2011թ.-ին TLD-ի հովանավորությամբ: Այս որոշումը նաև վերաբացեց հասարակական-քաղքաքական հարցերում ICANN-ի դերի քննարկումը:

Այլ հակադրություններ կարող են առաջանալ կապված gTLD-ի մշակութային և լեզվական միությունների հետ: 2003թ.-ին ICANN-ը ներմուծեց նոր .cat դոմեյնը կատալոնական լեզվի համար, որն առաջին դոմեյնն էր՝ ներմուծված լեզվի համար: Այս որոշմանը իսպանական կառավարությունը դեմ չէր, սակայն կարող են լինել դեպքեր, երբ լեզվական և մշակութային միվորումները, որոնք նույնն են ցանկանում, պետականացման ձգտումներ ունենան, և այս բնագավառը կարող է պոտենցիալ հակասությունների և կոլֆլիկտների պատճառ հանդիսանալ:

Ազգային դոմենների կառավարումը

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 Փոսթելը14: 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 մոտեցումներ15: 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 ընթացակարգը16: 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:

Միջազգայնացված 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 (International-ised 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» սերվերներ (Root սերվերներ)

«Արմատական» սերվերները, 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 սերվերները անջատվելու են և համացանցը դադարելու է աշխատել: Նախ՝ գոյություն ունի 13 արմատական սերվեր, 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 սերվերներում: 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 սերվերները կամ ստեղծել նորերը: Միաժամանակ արմատական սերվերների 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 սերվերներ 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 սերվերների վրա, որը առևտրի նախարարության հետ կնքած պայմանագրի համաձայն, գտնվում է VeriSign ընկերության ղեկավարման ներքո: Հիմնական արմատական սերվերների 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 սերվերների 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 սերվերների 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 վերանայվել է 2011 թ. և ԱՄՆ կառավարությունն IANA-ի համար առաջարկեց նոր պայմանագիր սկսել 2012թ.-ի ապրիլի 1-ից: : 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 սերվերներ. հնարավորություններ ու սահմանափակումներ

Այլընտրանքային արմատական սերվերների 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:

Գաղափարական քննարկում. մեկ root սերվերների համակարգն ընդդեմ այլընտրանքայինի

Երկար ժամանակ մեկ root սերվերի սկզբունքները համարվում էին Համացանցի հիմնական կառուցվածքը, որի մասին նույնիսկ չէր ենթադրվում քննարկում: Տարբեր փաստարկներ էին առաջ գալիս այլընտրանքային root սերվերի վերաբերյալ որևէ քննարկում սկսելը կանխելու համար: Մեկ փաստարկն այն էր, որ ներկա համակարգը կանխարգելում է DNS-ը կառավարական գրաքննության ենթարկելու ռիսկերը: Այս

տեսա-կետը հաճախակի է ներկայացվում ԱՄՆ պաշտոնյաների կողմից, իսկ այլ ոչ ամերիկյան հզոր Համացանցի կառավարման միավորումներ ընդդիմանում են վերջինիս: Այնուամենայնիվ, գրաքննության ենթարկվելու փաստարկը ֆունկցիանալության հիմքում զիջում է իր դիրքերը: Կառավական մարմինները գրաքննություն ներմուծելու համար DNS համակարգը կամ root գոտին վերահսկելու կարիք չունեն: Նրանք հիմնվում են ավելի արդյունավետ միոցների վրա՝ ֆիլտրելով Web հոսքը:

Առավել ծանրակշիռ փաստարկն այն է, որ այընտրանքային root սերվերները կարող են ֆրագմենտացիա առաջացնել և նույնիսկ բերեն Համցանցի վերջնական կործանման՝ ներառյալ հնարավոր բռնի կործանման սցենար: Համացանցի ֆրագմենտացիան կարող է վտանգել Համացանցի հիմնարար ֆունկցիաներից մեկը՝ գլոբալ միասնական հաղորդակցման համակարգը: Ինչքան իրատեսական է այս վտանգը: Վիտորիո Բեռտոլան առաջարկում է այս մարտահրավերի չափազանց բարդ վերլուծություն:

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:

Ցանցի չեզոքությունը

Համցանցի հաջողությունը կայանում է վերջինիս դիզայնի մեջ, որը հիմնված է ցանցի չեզոքության սկզբունքի վրա: Ի սկզբանե, Համացանցում բավանդակության հոսքն, անկախ այն գալիս էր սկսնակ կամ մեծ կազմակերպություններից, դիտարկվում էր առանց որևէ խտրականության: Նոր կազմակեր-պությունները և նորարարները թույլտվության կամ շուկայում իշխանության կարիք չունեին Համցանցում նորարարություն կատարելու համար: Այս հարցը գրավեց մի շարք գործող անձանց. սկսած ԱՄՆ նախագահից մինչև Մարդու իրավունքների պաշպանության ակտիվիստների: Համացանցի չեզոքության սկզբունքը ապագայում կարող է մեծ ազդեցություն ունենալ Համացանցի զարգացման վրա:

Ներկա իրավիճակը

Սկսած Dial-up մոդեմների վաղ ժամանակաշրջանից՝ մրցակցություն է եղել հնարավոր թողունակության և օգտատորորին անհրաժեշտ թողունակության միջև: Այս մարտահրավերը հաղթահարելու համար Համացանցի օպերատորները սկսել են կիրառել թրաֆիկի կառավարման տեխնոլոգիաներ: Օրինակ՝ համացանցի թրաֆիկի կոնվերտացումը VoIP-ի ծառայությունների շուրջ պետք է առաջնահերթություն ունենա հասարակ e-mail թրաֆիկի նկատմամբ. Skype-ով խոսալու ընթացքում ձայնի ուշացումը նկատելի կլինի, մինչդեռ e-mail-ի թրաֆիկի փոխանակման պարագայում փոքր ուշացումները մենք չենք նկատի: Թրաֆիկի կառավարման անհրաժեշտությունը հատկապես կարևոր

է ներկա բարձր թողունակության պահանջի պարագայում. օգտատերերի աճող մեծամասնությունը օգտագործում են Համացանցի ձայնային և վիդեո զանգեր, խաղում են առցանց խաղեր, դիտում են հեռուստաշոուներ, ֆիլմեր բարձր HD որակով: Բացի այդ, անլար սպոկտորի տեխնիկական սահմաններին զուգընթաց անլար թողունակությունը դառնում է ավելի սակավ: Թրաֆիկի կառավորումը գերբեռնվածության, ուշացումը կանխելու տեսանկյունից դառնում է ավելի բարդ: Առաջին տարածայնությունները ցանցի չեզոքության սկզբունքների հարցում կայանում է նրանում՝ արդյոք ցանկացած թրաֆիկը պետք է ամբողջովին թույլատրված լինի: Ցանցի չեզոքության կողմիակից-ները պնդում են, որ բոլոր բիթերը ստեղծվում են հավասար ձևով և Համացանցի թրաֆիկը ևս պետք է մշակվի հավասաության սկզբունքով: Հեռահաղորդակցությունն ու պրոյադերները վիճարկում են, որ օգտատերերը պետք է ունենան Համացանցի ծառայություններին հավասար հասանելիություններ, և եթե դա տեղի է ունենում, ապա Համացանցի թրաֆիկը չի կարող հավասարապես մշակվել: Եթե և՛ վիդեո, և՛ e-mail թրաֆիկները մշակվեն հավասարապես, ապա օգտագործողները չեն ունենա վիդեոհոսքի լավ ընդունելու հնարավորություն, մինչդեռ e-mail-ի մի քանի վայրկյան ուշացումը նկատելի չի լինի: Նույնիսկ ցանցի չեզոքության կողմնակիցները այս հիմնավորման վրա չկասկածեցին: Նրանք մտահոգվում են, որ որևէ զիջում ցանցի չեզոքության բնագավառում կարող է բացել «Պանդորայի արկղը»՝ առաջացնելով թրաֆիկի հիմնավորված կառավարման և հնարավոր շահարկման խնդիրը:

Թողունակության աճող պահանջարկ

2009թ.-ին թողունակության աճող պահանջարկը ցուցադրելու համար, YouTube-ի այցելուները դիտում էին 1.2 միլիարդ վիդեո մեկ օրվա ընթացքում և վերբեռնում էին ավելի քան 20 ժամանաց վիդեո յուրաքանչյուր րոպե:

Հարցեր

Ցանցի չեզոքության քննարկման շրջանակներում առաջ է գալիս այն համոզմունքը, որ անհրաժեշտ է թրաֆիկի

համապատասխան կառավարում իրականացնել: Հիմնական հարցը կայանում է նրանում՝ ինչպես մեկնաբանել «համապատասխան» բառը: Բացի տեխնիկական տեսանկյունից, գոյություն ունեն ևս երեքը՝ տնտեսական, օրինական և մարդու իրավունքների:

Տնտեսական հարցեր

Անցյալ մի քանի տասնամյակի ընթացքում ցանցային շատ կարևոր օպերատորներ՝ ներառյալ կապի օպերատորները և պրովայդերները, փոխել են իրենց բիզնես մոդելները. բացի ֆիզիկական և իրավաբանական անձանց համացանցին հասանելիություն տրամադրելուց, վերջիններս ներմուծել են իրենց սեփական VoIP-ն և IP հեռուստատեսությունը, երաժշտություն կամ վիդեո բեռնելու պորտալները և այլն: Այժմ նրանք մրցում են ոչ միայն ավելի մատչելի, արագ և բարձր որակի կապ մատակարարելու գծով, այլև «բարձրագույնից վերև» (over-the-top OTT) սկզբունքին համաձայն:

Թրաֆիկի կառավարումը կարող է կարևոր միջոց հանդիսանալ, երբ համեմատում ենք ծառայության և բովանդակության մատակարարողներին՝ ըստ փաթեթների փոխանցման բիզնեսի նախապատվութ-յունների: Օրինակ՝ օպերատորը կարող է որոշել դանդաղեցնել կամ ամբողջովին դադարեցնել այլ մրցակից կազմակերպությունների փաթեթների հոսքը՝ մյուս կողմից նախապատվությունը տալով իր ներքին ծառայություններին: Միևնույն ժամանակ, օպերատորները վիճում են, որ թողունակության պահանջի ընդլայնումը ծառայում է հիմնական կառուցվածքի ներդրումների աճին: Դիտարկելով OTT ծառայության մատակարարողներին որպես պահանջարկի ընդլայնման մեջ ամենից շատ ներդրում ունեցող և բարելավված կառուցվածքից ամենից շատ շահում ունեցող կողմ, նրանք առաջարկում են բազմամակարդակի ցանցի քաղաքականության մոդելը, որը ենթադրում է OTT ծառայության պրովայդերներից կողմից գումարի վճարում, եթե վերջիններս ծառայության համար երաշխավորված որակ են ցանկանում են: Այս պարագայում թրաֆիկի կառավարումը կրկին ավելի շատ կօգտագործվի տնտեսական, քան տեխնիկական նկատառումներից ելնելով: Նման քաղաքականության մոդելը, որը խախտում է ցանցի չեզոքության սկզբունքը,

ETNO-ն է՝ Եվրոպայի հեռահաղորդակցության ցանցի ասոցիացիան, առաջարկում է բազմամակարդականի ցանց «ուղարկողը վաճարում է» սկզբունքով: Այն հանդիսանում է1988 ITR-ի վերանայված տարբերակը, որը ներկայացվել է 2012թ.-ի WCIT-12-ի շրջանակներում Դուբայում: Տարիներ շարունակ բազմամակարդականի Համացանցի վերաբերյալ առաջարկությունները ցանցի չեզոքության մասնին քննարկումների կենտրոնում են եղել: 2010թ.-ին բիզնես շրջանակներում Verizon-ի և Google-ի կոմից ևս առաջարկվել են «լրացուցիչ առցանց ծառայություններ» (Բաց Համացանցի համար օրենսդրական հենքի առաջարկ): Կողմնակիցները պնդում են, որ սա օգտատերերի համար մեծ ընտրություն կստեղծի և կխրախուսի կառուցվածքում ներդրում-ները, ընդդիմադիրները վախենում են, որ ցանցը կտուժի և ի վերջո կանհետանա, քանի որ թե՛ բիզնեսը, թե՛ տնտեսությունը արդյունավետորեն կօգտագործեն նույն խողովակը:

Բազմամակարդականի Համացանց

Ներկայումս Համացանցը մատակարարվում է «ողջ ջանքերով». այն իրականացվում է առանց QoS-ի, արդյունարար արագության կամ փաթեթների ստացման ժամանակի երաշխավորման: Փոխարենը օգտագործողները բաշխում են հասանելի թողունակությունը և ստանում բիթային դրույքներ(արագություն) կախված ժամանակի ընթացքում երթևեկության բեռնվածությունից: Հետևաբար երթևեկության կառավարումը կարևոր դեր է խաղում ծառայության արդյունավետ որակի վրա վերջնական օգտագործողի համար:
Բազմամակարդականի Համացանցի գաղափարը ենթադրում է «բիզնես մակարդակի» ներմուծում, օրինակ՝ հատուկ ծառայություններերաշխավորված QoS-ի առկայությամբ: Կաղմնակիցները բացատրում են, որ բիզնես-մակարդակը կգործի տնտեսական-մակարդակին զուգընթաց, որը կհիմնվի ողջ ջանքերի ներդրման վրա, բացի այդ OTT ծառայության մատակարարաները կարող են որոշել ներդնել իրենց ողջ ջանքերը առանց արժեքի, եթե ցանկանան:

Իրավական հարցեր

Համացանցի կառավարման մեկ այլ խնդիր է հանդիսանում Համացանցի օպերատորների կողմից այն-պիսի նյութերի բլոկավորումը, որը կարող է հեղինակային իրավունքի

խախտման հանդիսանալ: Արդյո՞ք պրովայդերները թրաֆիկը կանգնեցնելու իրավունք կամ պարտականություն ունեն, օրինակ՝ P2P ցանցերում, որոնք նախատեսված են հեղինակային իրավունքների մասին նյութերը տարածելու համար: Արդյո՞ք նրանք իրավական և ադմինիստրատիվ մարմիններ ունեն, որոնք իրավասու են նման գործողությունների համար: Այս հարցերից որոշները եղել են Դաշնային հեռահաղորդակցության միության (FCC) և Comcast համացանցի օպերատորի միջև ծագած գործի ուշադրության կենտրոնում: 2007թ.-ին հասարակական շահերի պաշտպանության երկու խմբեր դիմում են FCC ԱՄՆ-ի կարգավորող մարմնին՝ պնդելով, որ Comcast օպերատորը խախտել է ցանցի չեզոքության սկզբունքը՝ էականորեն դանդաղեցնելոք BitTorrent ծրագիրն իր օգտագործողների համար:

Մարդու իրավունքներին վերաբերող հարցեր

Ցանցի չեզոքության սկզբունքի խախտման հետևանքները միայն տնտեսական չեն: Համացանցը կարևոր է դարձել ոչ միայն տնտեսական տեսանկյունից. այն դարձել է ժամանակակից հասարակության առանցքային սյուներից մեկը, որը կապված է մարդու իրավունքների հետ՝ ներառյալ տեղեկատվությանը հասանելիություն, արտահայտվելու ազատություն, առողջություն և կրթություն: Ի տարբերություն այլ տեխնոլոգիաների՝ Համացանցն ունի օգտատերեր, այլ ոչ թե սպառողներ: Ամբողջությամբ շահույթով առաջնորդվող մոդելները կարող են մեծացնել բաժանումը ունևորների և չունևորների միջև. մինչդեռ հարուստները օգտագործում են անսահմանափակ առցանց ծառայություններ ամբողջական որակով, աղքատներին ի վերջո տրամադրվում են սահմանափակ ծառայություններ: Հետևաբար, վտանգելով Համացանցի բաց լինելը, եմնք վտանգում ենք Մարդու հիմնարարա իրավունքները: Բացի այդ, ցանցի թրաֆիկն ըստ վերջինիս ծագումն կամ նշանակակետի, ծառայության կամ բովանդակության կառավարելու կարողությունը կարող է կառավարությանը հնարավորություն ընձեռել զտել Համացանցի թրաֆիկն՝ ըստ դատապարտելի կամ զգայուն բովանդակության՝ կախված պետության քաղաքական, գաղափարական, կրոնական, մշակութային և այլ արժեքներից: Սա կարող է թրաֆիկի կառավարման գրաքննության ռիսկ

ներկայացնել, հատկապես այն երկրներում, որտեղ ավտորիտար ռեժիմ է տիրում:

Ռիսկերը

Եթե թրաֆիկի կառավարումը դուրս գա Համացանցի բոլոր օգտագործողներին հավասար ծառայություններ մատակարարելու համապատասխան մակարդակից, ապա ցանցի չեզոքության սկզբունքը կվտանգվի: Դա կարող է առաջ բերել բազմամակարդականի Համացանցի առաջացմանը: Համաձայն «Պահպանեք Համացանցը» և «Համացանցի կառավարման միավորում» օգտատերերի խմբի՝ Համացանցը կարող է դառնալ պրովայդերների կողմից առաջարկվող առևտրային փաթեթների հավաքածու, որում օգտատերերը կարող են ունենալ միայն կոնկրետ ընտրված փաթեթի ներսում կոնկրետ առցանց ծառայությունների և բովանդակության հասանելիություն: Ըստ այդմ, նրանք նախազգուշացնում են, որ եթե օպերատորները սկսեն փոփոխել բովանդակությունը կամ ծրագրերը, ապա դա կոչնչացնի օպերատորների ծառայությունների մրցակցությունը և կվտանգի փոքր բիզնեսը, սկսնակներին և ոչ առևտրային առաջարկները, ինչպիսիք են հաշմանդամների համար նախատեսված ծրագրերը, որոնք սովորաբար բարձր թողունակություն են պահանջում:

Օգտագործողնե՞ր, թե՞ հաճախորդներ

Ցանցի չեզոքության բանավեճը առաջ է քաշում նաև լեզվական քննարկումներ: Ցանցի չեզոքության կողմնակիցները կենտրոնանում են Համացանցի օգտագործողների վրա, մինչդեռ մյուսները՝ հատկապես կոմերցիոն մասնակիցները, նկարագրում են վերջիններիս որպես հաճախորդներ: Համացանցի օգտագործոսները ավելին են, քան պարզապես հաճախորդներ. «օգտատեր» տերմինը ենթադրում է Համացանցի զարգացման մեջ ակտիվ մասնակցություն սոցիալական ցանցերի, բլոգերի և այլ գործիքների միջոցով, ինչպես նաև Համացանցի ապագայի որոշման հարցում կարևոր դեր ունեն: Մյուս կողմից, հաճախորդները, ինչպես ցանկացած այլ բնագավառի հաճախորդ, կարող են որոշել վճարել առաջարկված ծառայության համար, թե՝ ոչ: Նրանց վիճակը հիմնված է ISP-ի հետ կնքված պայմանագրի և հաճախորդների իրավունքների պաշտպանության վրա: Բացի այդ, հաճախորդներն իրավունք չունեն որոշելու՝ ինչպես է Համացանցը աշխատում:

Ովքեր են գլխավոր դերում և որո՞նք են նրանց փաստարկները

Հիմնական խաղացողների դիրքը մշտապես գտնվում է տեղաշարժման վիճակում: Օրինակ՝ Google-Verizon 2010թ.-ի ցանցի չեզոքության միջանկյալ մոտեցման առաջարկը տեղաշարժեց հիմնական խաղացողների դիրքերը: Google-ը հանդիսանում էր ցանցի չեզոքության հիմանական կողմակիցներից, մյուսն կողմակիցներից են սպառողների պաշտպանները, առցանց կազմակերպությունները, որոշ տեխնիկական կազմակերպություններ, հիմնական Համցանցային ծրագրերի կազմակերպություններ՝ ներառյալ Yahoo!, Vonage, Ebay, Amazon, EarthLink, և ԾԱ կազմակերպություններ, ինչպիսին է Microsoft-ը: Ցանցի չեզոքության ընդդիմադիրները ներառում են կապի ընկերությունները, պրովայդերները, ցանցային սարքավորումների և ապարատային միջոցների արտադրողները, վիդեո և մուլտիմեդիա նյութեր արտադրողները: Նրանց փաստարկներն ընդդեմ ցանկացած կարգավորման շուկայական կենտրոնացում ունեն՝ սկսած անհրաժեշտությունից՝ ինչ է սպառողը ցանկանում: Ի հեճուկս կապի օպերատորների՝ ցանցի չեզոքության նկատմամբ ցանկացած կարգավորման դեմ լինելու ընդհանուր միտումների՝ ETNO-ի առաջարկը WCIT12-ին եղավ միջազգային կարգավորումը, ինչը ենթադրում էր ապագայում պաշտպանել ցանցի չեզոքությունը ազգային կարգավորումից: Նրանց ԱՄՆ-ի գործընկեր-ները, օրինակ՝ Verizon-ը, այնուամենայնիվ, դեմ էին ETNO-ի նախաձեռնությանը:

Ցանցի չեզոքության քննարկումներում գոյություն ունեն չորս հիմնական փաստարկներ.

Փաստարկ	Ցանցի չեզոքության համակիրներ	Ցանցի չեզոքության ընդդիմադիրներ
Անցյալ/ ապագա	Շնորհիվ Համացանցի բաց ճարտարապետության՝ նոր Համացանցային կազմակերպություններ են ստեղծվել, և շնորհիվ ցանցի չեզոքության՝ վերջավոր օգտագործողները շահում են ծառայությունների անվերջանալի բազմազանությունից: Ցանցի չեզո-քությունը կպահպանի Համացանցի ճարտարապետութ-յունը, ինչը նպաստել է Համացանցի արագ և նորարարկան զարգացմանը:	Թրաֆիկի կառավորումն անխուսափելի է, և չեզոքություն երբեք գոյություն չի ունեցել: Բացի այդ, արդեն իսկ գոյություն ունեն ոչ չեզոք ծառայություններ, ինչպիսին VPN-ն է: Առանց ցանցի չեզոքության սահմանա-փակության Համացանցի կազմակեր-պությունները կարող են երաշխավոր-ված QoS-ով նոր ծառայություններ զարգացնել, որոնցում հաճախորդները հետաքրքրված կլինեն:
Տնտեսական	Առանց ցանցի չեզոքության Համա-ցանցը կնմանվեր կաբելային հեռուստատեսության. մի բուռ խոշոր կազմակերպություններ կկա-ռավարեին բովանդակության բաշ-խումը և հասանելիությունը՝ որոշելով՝ օգտագործողները ինչ պետք է տեսնեն և որքան դա կարժենա: Սկասնակները և փոքր բիզնեսի ներկայացուցիչները զարգացման հնարավորություն չեն ունենա, հատկապես զարգացող երկրներում:	Առանց ցանցի չեզոքության սահմանա-փակման բովանդակության և ծառա-յությունների պրովայդերների հետ առևտրային համաձայնագրերում կապի օպերատորները կբարձրացնեին միջոցներ, ինչը նրանց ավելի հետաքրքրված կդարձներ ավելի լավ կառուցվածքում ներդրում կատարելու մեջ: Ավելի լավ ենթակառուցվածքը կխրախուսեր նոր՝ հաճախորդի պա-հանջներին ավելի հարմարեցված ծառայությունները և նորարարութ-յունները: OTT ծառայությունների պրովայդերները ևս կարժևորեն QoS-ով հնարավոր նորարական ծառայութ-յուններ:

Էթիկական	Համացանցը բազմաթիվ կամա-վորականների տասնամյակների մշակման արդյունք է: Նրանք ժամանակ և ստեղծագործական միտք են ներդրել Համացանցում ամեն ինչ զարգացնելու համար՝ սկսած տեխնիկական պարատա-կոլներից մինչև բովանդակություն: Համացանցը ավելին է, քան բիզնեսը. այն դարձել է մարդկության գլոբալ ժառանգութ-յուն: Դա արդարացված չի լինի ունենալ այսպիսի հսկայական ժամանակի և ստեղծագործական մտքի ներդրում, որը բարիքները քաղում են միայն մի քանի կազմակերպություններ, որոնք բլոկավորում են Համացանցը բիզնեսի հարկադրական մոդելնե-րում՝ խախտելով Համացանցի չեզոքությունը և ամբողջ ջանքերը շահույթի վերածելով:	Համացանցի չեզոքությունը էթիկորեն կասկածելի է, քանի որ օպերատորները ստիպված են ներդրում կատարել Համացանցի ենթակառուցվածքի պահպանման և ընդլայնման համար նոր ծառայություններն աջակցելու նկատառումներից ելնելով, մինչդեռ շահույթի մեծ մասը բաշխվում է այնպիսի բովանդակային կազմակեր-պությունների միջև, ինչպիսին Google-ը, Facebook-ը կամ Amazon-ն է:
Կարգավորման	Ցանցի չեզոքությունը պետք է կիրառվի կառավարության կողմից հասարարկական շահերը պաշտպանելու համար: Ցանկացած ինքնակարգավորում այս հարցը բաց կթողնի օպերատորների համար, որոնք կխախտեն ցանցի չեզոքութ-յան սկզբունքը: Բաց շուկան բավարար մեխանիզմ չէ, քանի որ հիմնական գլոբալ կապի օպերատորները Համացանցի ենթակառուցվածքի միջուկում են: Բացի այդ ընտրություն կայացնելն այդքան հեշտ և հասանելի չէ նույնիսկ օպերատորների ամբող-ջովին թափանցիկ առաջարկների դեպքում:	Համացանցը զարգացել է, քանի որ կարգավորումը կամ թեթև է եղել կամ բացակայել է: Կառավարական ծանր կարգավորումները կարող են խեղդել ապագայում ստեղծագործական զարգացումը: Բաց շուկան հիմնված է ընտրության վրա, և օգտատերերը միշտ կարող են փոխել իրենց պրովայդերներին, եթե առաջարկով բավարարված չեն: Օգտատերերի ընտրությունը կսպանի վատ առաջարկները և կպահպանի լավագույնները:

Հիմնական սկզբունքները

Վերջին տարիներին ցանցի չեզոքության վերաբերյալ քննարկումներն ու կարգավորումները վերջինիս համար կերտել են մի քանի հիմնարար սկզբունքներ.

- Թափանցիկություն. օպերատորները պետք է մատակարարեն ամբողջական և ճշգրիտ տեղեկատվություն իրենց ցանցային կառավարման փորձի, հզորության, որակի վերաբորյալ այնպիսի ձևաչափով, որը հասկանալի է միջին օգտագործողին:
- Հասանելելություն. օգտատերերը պետք է ունենան հասանելիություն ցանկացած բովանդակության, ծառայության, ծրագրի կամ կարողանան միանալ ցանկացած սարքավորման, որը ցանցի աշխատանքին չի վնասում:
- (Ոչ) խտրականություն. օպերատորները պետք է խտրականություն չդնեն թրաֆիկի վրա հիմնվելով.
    - ուղարկողի կամ ստացողի ծագման վրա,
    - բովանդակության, ծրագրի և ծառայության տեսակի վրա,
    - որտեղ ողջամիտ կարող է լինել ցանկացած հասարակական շահ և ոչ միայն բիզնեսի նկատառումներց:

Այլ սկզբունքներ, որոնք հաճախակի են քննարկվում միջազգային ֆորումներում, ինչպիսիք են IGF հանդիպումները և EuroDIG երկխոսությունը, ներառում են.

- ազատ արտահայտման, տեղեկատվությանը հասանելիության և ընտրության պահպանում,
  ծառայության մինիմալ որակի, անվտանգության և ցանցի ճկունության ապահովում,
- ներդրումների խթանման պահպանում,
- նորարարություն խթանում,
- ներգրավված բոլոր կողմերի իրավունքների, դերերի և պատասխանատվությունների սահմանում, ներառյալ բողոքարկման և փոխհատուցման իրավունքները,
- հակամրցակցային պրակտիկայի կանխարգելում,
- շուկայական միջավայրի ստեղծում, որը թույլ կտա օգտատերերին հեշտորեն ընտրել և փոխել իրենց ցանցի օպերատորներին,
- անապահով անձանց, ինչպիսիք են հաշմանդամները, զարգացող երկրների օգտատերերի և բիզնեսի շահերի պաշտպանում,

- բովանդակության և ծառայության բազմազանության պահպանում:

Քաղաքականության մոտեցում

Ցանցի չեզոքությանը զուգընթաց ծագում է այլ հարց է ծագում. ինչ է լայնաշերտ քաղաքականության կարգավորման և օպերատորների փորձի դերը: Գլխավոր մարտահրավերներից մեկը, որին դեմ են առնում կարգավորողները, այն է՝ արդյոք գործեն վաղօրոք, որպեսզի կանխեն ցանցի չեզոքության հնարավոր խախտումները, թե պատասխանեն՝ հիմնվելով նախադեպերի վրա, երբ մեկ անգամ խախտում կատարվի: Մյուս մարտահրավերը կայանում է նրանում՝ արդյոք խնդրով պետք է զբաղվել «ծանր օրենքների» շրջանակներով՝ սկզբունքները կիրառելով օրենսդրության մեջ, թե՝ «թեթև օրենքը» բավարար կլինի:

Զարգացած երկրներ

Ի պատասխան Comcast-ի գործի՝ ԱՄՆ-ի FCC-ն, որպես 2005թ.-ի իր քաղաքականության թարմացում, ընդունեց ցանցի չեզոքության վերաբերյալ ուղեցույցներ, որն արտացոլում էր բովանդակության ու սարքավորումների ընտրության և հասանելիության անհրաժեշտությունը՝ անդրադառնալով խտրակա-նության և թափանցիկության հարցերին: Ճապոնիայի Ներքին ազդեցությունների և հեռահաղորդակցության աշխատանքային խումբը զեկուցեց ընտրության և հասանելիության, ինչպես նաև խտրականության մասին՝ լրացուցիչ կերպով անդրադառնալով ցանցի արժողության բաշխվածությանը: Շվեդական Փոստի և կապի գործակալությունը (PTS) նշեց, որ հրապարակայնութ-յունը, որին նպաստում է անխտրականությունը և մրցակցությունը, նորարարության նախապայման է, բայց նաև այն պետք է հավասարակշռվի ցանցի ներդրումներով և անվտանգությամբ: Էլեկտրոնային հեռահաղորդակցության ԵՄ կարգավորումը կենտրոնանում է ազատ արտահայտման, օգտատերերի ընտրության և հասանելիության իրավունքի պաշտպանության վրա, ինչպես նաև թափանցիկության սկզբունքի վրա՝ միևնույն ժամանակ ընդգծելով ներդրումների, առանց խտրականության արդար մրցակցության և նոր բիզնես մոդելների

հնարավորությունների անհրաժեշտության վրա: 2011թ.-ի հունիսին Նիդեռլանդները դարձավ առաջին Եվրոպական երկիրը, որը ցանցի չեզոքության սկզբունքն արձանագրեց ազգային օրենսդրությունում: Ամենից գովելի մոդելը Նովեգիայի Փոստի և հեռահաղոր-դակցության ղեկավարության(NPT) առաջարկն էր, որի նպատակն էր բիզնես առաջարկների թափանցի-կությունը և փորձը, օգտատերերի ընտրությունը և բովանդակության հասանելիությունը, ծառայությունները և սարքավորումները, ինչպես նաև ծրագրերի, ծառայությունների, բովանդակության, ուղարկողի և ստացողի անխտրականությունն ապահովելը: Այնուամենայնիվ, միայն բովանդակությունը չէ, որ առանձնանում է, բարց նաև այս ուղեցույցների առումով համաձայնության հասնելու պրոցեսն այն եղանակով, որ NPT-ն կրկիին երաշխավորում է սպառողներին և բիզնեսին շուկան առանց ցկոշտ¦ օրենքի կարգավորվելու հնարավորությունը: Որոշ երկրներ, ինչպիսին են Ավստրալիան, Նոր Զելանդիան, այնուամենայնիվ, չեն կանխում բիզնեսկողմորոշված խտրականությունը, և հետևաբար համարվում են ցհակաչեզոքական¦ կղզիներ, որտեղ կարելի է տեսնել՝ ինչ են իրենցից ներկայացնում Համացանցի ոչ չեզոք հեռանկարները:

Զարգացող երկրներ

Ենթակառուցվածքի և թողունակության շնորհիվ՝ զարգացող երկրներում կարգավորողներն ավելի շատ կենտրոնանում են քաղաքականության արադր օգտագործման վրա. մատչելի գներ և արդար հասանե-լիություն բոլորի համար: Որոշները մտահոգվում են միջսահմանային անխտրականության շուրջ՝ նշելով, որ թրաֆիկը բոլոր երկրներից պետք է մշակվի նույն ձևով առանց հիմնվելու գների առաջնահերթության վրա: Որոշ երկրներ նաև մտահոգվում են ներքին մշակութաին, քաղաքական կամ այլ էթիկական կող-մերի վերաբերյալ, հետևաբար համապատասխան օգտագործման և կառավարման հասկացողություն-ները տարբերվում է մյուսներից: Կային նաև մտորումներ այն հարցի շուրջ, որ զարգացած երկրների նորարական մոդելները կարող են խոչընդոտել զարգացող երկրների շուկան՝ նախապատվությունը մեծ արևելյան կազմակերպություններին տալով, առաջացնելով բիզնես և լրացուցիչ կրճատված մրցակցութ-յուն, սպառնալով

բազմազանությանը և նորարարությանը: Այնուամենայնիվ, մի քանի հիմական պաշտո-նական քաղաքականություններ կամ կարագավորումներ ցանցի չեզոքության վերաբերյալ, եկել են զարգացող աշխարհից, որոնցից մեկը Չիլիի ցանցի չեզոքության վերաբերյալ 2010թ.-ի ազգային օրենքն է:

Միջազգային կազմակերպությունները և NGO-ները

Մի շարք միջազգային կազմակերպություններ և օգտատերերի խմբեր ևս մշակել են ցանցի չեզոքության վերաբերյալ քաղաքականություն: ԵԽ-ն 2010թ.-ի ցանցի չեզոքության վերաբերյալ Նախարարների հռչակագրի կոմիտեի շրջանակներում ընդգծում է ազատ արտահայտման հիմնարար իրավունքները, Համացանցի միությունն(ISOC) առաջարկում է իր օգտատերակենտրոնացված մոտեցումը, որը մեծամա-սամբ շոշափում է հասանելիության, ընտրության և թափանցիկության հարցերը §Բաց միջցանցային¦ քննարկման շրջանակներում: Սպառողների միձատլանտյան երկխոսությունը (TACD)՝ ԱՄՆ-ի և ԵՄ-ի սպառողների կազմակերպությունների ֆորումը լրացուցիչ կերպով ընդգծում է ոչ խտրական վարքագիծ ունեցողների հարցումների առկայությունը՝ կոչ անելով ԱՄՆ-ին և ԵՄ-ին հանդես գալ որպես օգտատե-րերի իրավունքների պաշտման: Ցանցի չեզոքության և Համացանցի բազմամակարդականի սկզբունքները լայնորեն քննարկվել են WCIT-12-ի շրջանակներում:

Շատ հասարարկակն կազմակերպություններ հատկապես մտահոգվում են ոչ առևտրային և ոչ մրցակցային առցանց բովանդակության և ծառայությունների ապագայի շուրջ՝ պահանջելով, որ վերջիններս լինեն հավասար ցանկացած այլ առևտրային: Նրանք նաև ընդգծում են խոցելի խմբերի իրավունքները, հատկապես հաշմանդամների կարիքները բովանդակությունը, ծառայությունները և ծրագրերն առանց որևէ սահամանափակումների օգտագործելու անհրաժեշտությունը:

Բաց հարցեր

Կան մի շարք բաց հարցեր ցանցի չեզոքության քննարկման օրակարգում.

- Որտե՞ղ պետք է լինի հավասարակշռությունը

Համացանցի հասարակական բարիքների մի կողմից և

մյուս կողմից օգտատերերի իրավունքների միջև, ինչպես նաև օպերատորների նորարարական իրավունքները ցանցի շրջանակներում,

- Արդյո՞ք չկարգավորված շուկան բաց մրցակցությամբ կլինի նույնքան պաշտպանված և օգտատերերի համար կմատակարարի անսահմանափակ ընտրություն: Եվ արդյո՞ք օգտատերերը ի վիճակի կլինեն իմաստալից որոշումներ կայացնել: Թե՞ կարգավորումը անխուսափելի է, և եթե այո, ապա ո՞ր մարմինը պետք է հանդես գա որպես կարգավորող:
- Ինչպե՞ս են տարբեր կարգավորման մոտեցումները ազդելու լայնաշերտ շուկայի և հետագա ներդրումների ու նորարության վրա:
- Որո՞նք են զարգացող աշխարհում ցանցի չեզոքության կիրառումները:

Որո՞նք են բազմամակարդականի Համացանցի համար մրցակցության, նորարաության, ներդրման և մարդու իրավունքների հետևանքները:

- Արդյո՞ք գերակշռող OTT բովանդակության և ծառայությունների պրովայդերները կդիտարկեն բազմամակարդականի Համացանցը և հնարավոր նոր ծառայությունները որպես շահութաբեր բիզնես: Ո՞ր պարագայում նրանք ի վիճակի կլինեն ներառել զարգացող երկրների օգտատերերին, թե՞ վերջիններս դուրս կմղվեն:
- Կարո՞ղ են արդյոք կապի օպերատորները նորամուծություն մտցնել իրենց բիզնեսում առանց ցանցի ներդաշնակությունը խախտելու:
- Արդյո՞ք թրաֆիկի կառավարումը տեխնիկական պատճառներով ապագայում կինանա՝ տեխնոլոգիական բարելավումների շնորհիվ:
- Ինչպե՞ս կազդի ամպային հաշվարկները կազդեն ցանցի չեզոքության քննարկումների վրա, և հակառակը:
- Արդյո՞ք թրաֆիկի կառավարումը կընդլայնվի (կրիչի մակարդակ) մինչև բովանդակության և ծրագրերի կառավարում (բովանդակության և ծրագրերի մակարդակ), ինչպիսի±նն են Google, Apple կամ Facebook:
- Արդյո՞ք սպառողների պաշտպանությունը կշարունակի ներքուստ կապված լինել ցանցի չեզոքությանը:
- Եթե ցանցի չեզոքությանը «պարտված» լինի, ապա ո՞ր սկզբունքները կպաշտպանեն սպառողներին ապագայում:

Համացանցի հասանելիություն. Համացանցային ծառայություններ մատակարարողները(ISP)

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 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 հիմնված 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 ներառում 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 հետ20:

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 տվեցին21:

Համացանցին հասանելիություն. լայնաշերտ համացանցային ծառայություններ մատակարարողները(IBSP)

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 համաձայնագրեր22: 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 մատակարարողներին23: 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:

Կարո՞ղ է հուսալիությունը լինել երաշխավորված

Արդյո՞ք հնարավոր է հիմնական հեռահաղորդակցման օպերատորներից Համացանցի գլոբալ միավորման համար պահանջել երաշխիք կամ հավաստիացում Համացանցի կրիտիկական ենթակառուցվածքների հուսալի ֆունկցիոնալության համար: Այս միտումը քննարկում է Համացանցի մասնավոր ենթակառուցվածքի օպերատորներին որոշակի հասարակական պահանջներ պարտադրելու հարցը:

Լայնագիծ կապի ծառայություններ մատակարարողները և կրիտիկական ենթակառուցվածքը

2008 թ. սկզբին Եգիպտոսից ոչ հեռու, Միջերկրական ծովում վնասվել 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 վնասվածքների 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

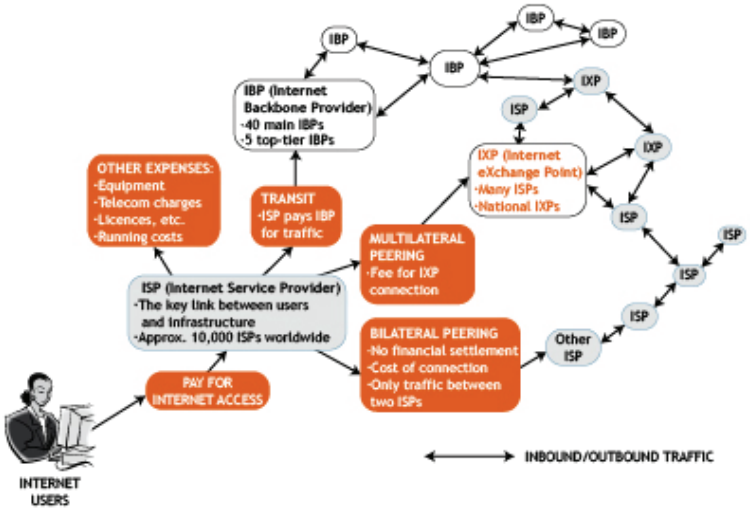
Մենք գիտենք, թե ինչպես կարգավորել փաթեթների փոխանցումը, սակայն չգիտենք, թե ինչպես կարգավորել դոլարների փոխանցումը:

Դավիթ Քլարկ

Արդի վիճակ

Համացանցի կառավարման հարցերի քննարկումը հաճախ շեշտադրում է շահույթի միջոցների և աղբյուրների բաշխման հիմնախնդիրը24: 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 միջև26: 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 շուկան27:

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 վրա28:

WEB 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

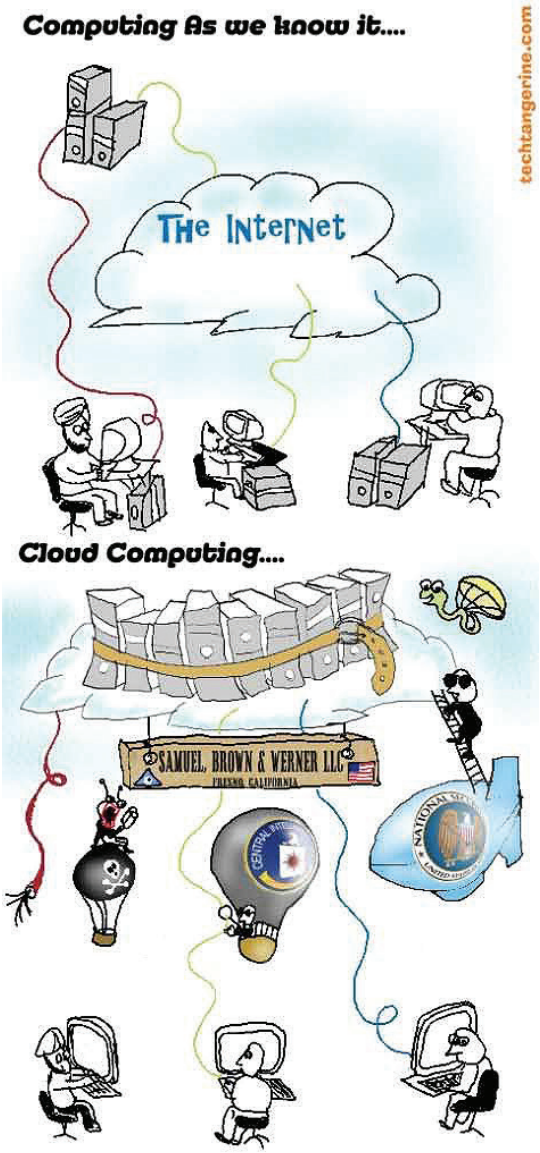
սարդոստայնի» (W3C) կոնսորցիումի շրջանակներում, որը ղեկավարում է Թիմ Բյոռնս Լին: Հետաքրքիր է, որ համացանցի կառավարման վերաբերյալ քննարկումներում W3C-ը, չնայած համացանցի համար իր մեծ կարևորությանը, դեռևս մեծ ուշադրություն չի գրավում:

«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): Face-book-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: Առաջին՝ 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, կկարողանա՞ն 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:

Հարցեր

Զուգամերձության տնտեսական հետևանքները

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 հենքի անհրաժեշտությունը

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:

Զուգամերձության ռիսկայնությունը. մալուխային օպերատորների միաձուլումը և համացանցային ծառայությունների մատակարարները

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 ĩնչ 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 հիմնախնդիրը 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:

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: Համագանցի անվտանգությանն առնչվող միջազգային իրավական կարևորագույն գործիք է 2004 թ. հուլիսի 1-ին ուժի մեջ մտած կիբեռհանցագործության վերաբերյալ ԵԽ համաձայնագիրը36: Որոշ երկրներ կնքել են նաև երկկողմանի պայմանագրեր: Քրեական հանցագործությունների հարցերով իրավական համագործակցության մասին ԱՄՆ-ն երկկողմանի պայմանագրեր է կնքել ավելի քան 20 երկրների հետ37: 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:

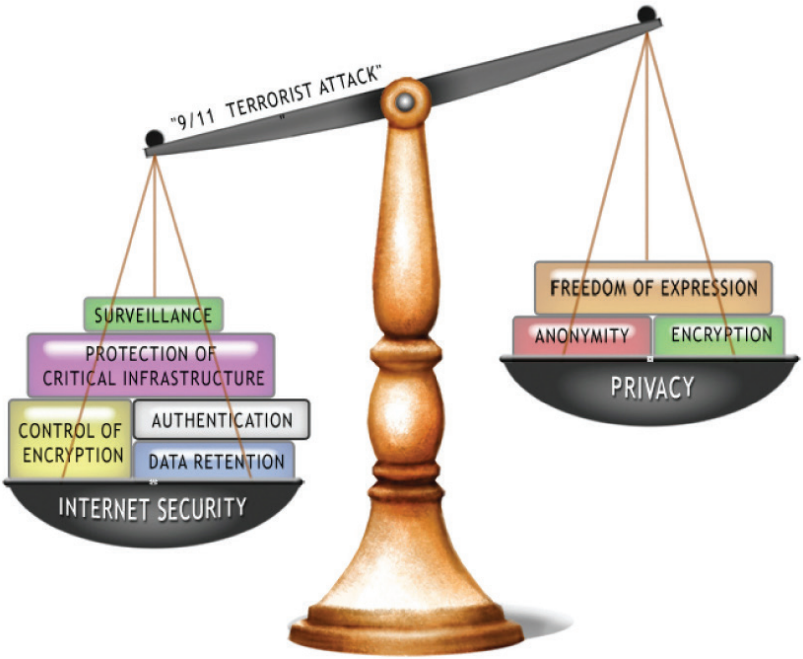
Հարցեր

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 գաղտնիությունը

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 գաղտնիության պաշտպանության 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 գաղտնիության 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 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 (ՏՀԶԿ, Organization for Economic Co-operation and Development, OECD): Վասենարյան պայմանագիրը 33 զարգացած երկրների հաստատած միջազգային կարգ է2, 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 ՏՀՁԿ-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(Սփամ)

Արդի վիճակ

Փոստաղբը սահմանվում է որպես փոստ ստացողի չսպասված 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 պոռնոգրական 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 նախաձեռնողականությունը39: 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:

Սփամ և «նորաձևության քաղաքականություն»

Սփամը միտումների, երբեմն գլոբալ քաղաքականության մեջ նորաձևության, ցուցադրական օրինակ է: 2005թ.-ին այն Համացանցի կառավարման կարևոր խնդիրներից էր, որը ներառված էր WGIG-ի՝ Համացանցի կառավարման հաշվետվության մեջ: Սփամը քննարկվել է WSIS-ի՝ Թունիսում կայացած և այլ բազմաթիվ միջազգային հանդիպումների շրջանակներում: Այն հաճախ լուսաբանվել է նաև մամուլում: 2005թ.-ից սկսած սփամի ծավալը եռապատկվել է՝ ըստ պահպանողական հաշվարկների(2005թ.՝ 30 միլիարդ հաղորդագրություն մեկ օրվա ընթացքում, 2008թ.՝ 100 միլիարդ, 2010թ.՝ 200 միլիարդ): Սփամի արդիականության քաղաքականությունը չի հետևում այս միտմանը: Ներկայումս գործընթացների գլոբալ քաղաքականության մեջ այն գրեթե տեսանելի չէ: 2009թ.-ի Շարմ Էլ Շեյխում կայացած IGF-ի ոչ մի հանդիպման կամ նիստի ժամանակ սփամը չի քննարկվել: Սփամի արդիականության քաղաքականությունն ակնհայտորեն դեռ պետք է բացահայտվի:

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 հիմնախնդիրը 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 հիմնախնդիրը

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 հիմնված լինի միջազգային պայմանագրի կամ համանման մի մեխանիզմի վրա: Ավստրալիայի, Կորեայի և Մեծ Բրիտանիայի համատեղ ստորագրած փոխըմբռնման հուշագիրը փոստաղբի դեմ պայքարի գործում 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, Earth-Link, 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 պոռնոգրաֆիական նյութեր) անուշադրության է մատնում: Երկրների մասում ղոստաղբ 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 The terms Internet and www are sometimes used interchangeably; however, there is a difference. The Internet is a network of networks connected by TCP/IP. Sometimes, the term Internet is used to encompass everything, including infrastructure, applications (e-mail, ftp, Web) and content. The www is just one of many Internet applications, a system of interlinked documents connected with the help of the HyperText Transfer Protocol (HTTP).

2 Following a policy of technological neutrality, the European Union has been using the term 'electronic communications' instead of 'telecommunications'. This covers, for example, Internet traffic over the electronic grid, which is not part of the telecommunications infrastructure.

3 Internet transfer via an electric grid is called Power Line Communication (PLC). The use of the power grid would make the Internet more accessible to many users. For a technical and organisational review of this facility, please consult: Palet J (2003) Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication, Internet Society, ISOC Member Briefing No. 13. Available at http://www.isoc.org/briefings/013 [accessed 18 January 2012].

4 The liberalisation of telecommunication markets of WTO members was formalised in 1998 in the so-called Basic Telecommunication Agreement (BTA). Following the adoption of BTA, more than 100 countries began the liberalisation process, characterised by the privatisation of national telecommunication monopolies, the introduction of competition, and the establishment of national regulators. The agreement is formally called The Fourth Protocol to the General Agreement on Trade in Services (adopted on 30 April 1996 and entering into force on 5 February 1998). Available at http://www.wto.org/english/ tratop_e/serv_e/4prote_e.htm [accessed 18 January 2012].

5 One of the controversies surrounding WSIS was the ITU's intention to become more involved in the Internet governance process, especially within a domain handled by ICANN. For more information about ITU's Internet policy, please consult http://www.itu. int/osg/spu/ip/ [accessed 14 March 2008].

6 For more information about the WTO's role in the field of telecommunications, please consult http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm [accessed 18 January 2012].

7 Latvia and Moldova are good examples of how it is possible to make a quantum leap forward in the quick development of a telecommunications infrastructure through the introduction of wireless communication; http://www.isoc.org/isoc/conferences/inet/99/ proceedings/4d/4d_2.htm [accessed 14 March 2008].

8 Initially the Wi-Fi Alliance was called the Wireless Ethernet Compatibility Alliance (WECA). It received its current name in 2002. It was established by

some of the leading developers of telecom equipment including: 3Com, Cisco, Intersil, Agere, and Nokia.

9 It is estimated that this investment totals approximately €109 billion, according to The Economist (2003) Beyond the Bubble Survey: Telecoms. Available at http://www.economist. com/node/2098913 [accessed 18 January 2012].

10 For more information about the EU radio spectrum policy see http://ec.europa.eu/ information_society/policy/ecomm/radio_spectrum_copy%281%29/sectorial/index_ en.htm [accessed 6 March 2012].

11 The current RIRs are: ARIN (the American Registry for Internet Numbers), APNIC (the Asia Pacific Network Information Centre), LACNIC (the Latin American and Caribbean IP Address Regional Registry), RIPE NCC (Reseaux IP Européens Network Coordination Centre – covering Europe and the Middle East) and AFRINIC (the African Network Information Centre). A detailed explanation of the RIR system is available at https://www. ripe.net/internet-coordination/internet-governance/internet-technical-community/ the-rir-system [accessed 26 January 2012].

12 For a detailed discussion on IPv6, please consult the research project: IP Allocation and IPv6 by Jean Philémon Kissangou, Marsha Guthrie, and Mwende Njiraini, part of the 2005 Internet Governance Capacity Building Programme. Available at http://archive1. diplomacy.edu/poolbin.asp?IDPool=130 [accessed 26 January 2012].

13 For a comprehensive and highly technical survey of TCP/IP Security, please consult: Chris Chambers, Justin Dolske, and Jayaraman Iyer, TCP/IP Security, Department of Computer and Information Science, Ohio State University. Available at http://www.linuxsecurity. com/resource_files/documentation/tcpip-security.html [accessed 25 January 2012].

14 One of the few referential documents on the Domain Name System (DNS) is RFC 1591 (March 1994), which specifies the governance structure of DNS.

15 An overview of the gTLDs with a link to the list of all the TLDs is available at http:// www.icann.org/en/resources/registries/about [accessed 2 March 2012].

16 The text of proposal is available at http://archive.icann.org/en/tlds/stld-apps-19mar04/xxx. htm; the retrospective of the .XXX application, within the minutes of the meeting of 30 March 2007 when it was rejected by the ICANN Board, is available at http://www.icann. org/en/groups/board/documents/resolutions-30mar07-en.htm#_blank [accessed 3 March 2012].

17 The US government did not use any ICANN procedure. It used its de facto authority via a letter sent by the US Department of Commerce to the Chairman of ICANN.

18 The application form for the registration of the .cat domain: http://archive.icann.org/en/ tlds/stld-apps-19mar04/cat.htm [accessed 3 March 2012].

19 The ITU's website contains a comprehensive bibliography of materials

related to Country Domain Management; most materials were delivered at the ITU Workshop on Country Domain Management held in Kuala Lumpur; http:// www.itu.int/ITU-T/worksem/ cctld/kualalumpur0704/contributions/index.html [accessed 25 January 2012].

20 The IANA Report on the county code top-level domain for Palestine is available at http:// www.iana.org/reports/ps-report-22mar00.htm [accessed 25 January 2012].

21 For example, South Africa used its sovereign rights as an argument in winning back control of its country domain. A newly enacted law specifies that the use of the country domain outside the parameters prescribed by the South African government will be considered a crime. The Brazilian model of the management of country domains is usually quoted as a successful example of a multistakeholder approach. The national body in charge of Brazilian domains is open to all key players, including government authorities, the business sector, and civil society. Cambodia's transfer of country domain management from non-governmental to governmental control is often cited as an example of an unsuccessful transition. The government reduced the quality of services and introduced higher fees, which have made the registration of Cambodian domains much more difficult. For more information, please consult: Alfonso C (2004) BR: CCTLD An asset of the commons, in MacLean D (ed) Internet Governance: A Grand Collaboration. New York: UN ICT Task Force, pp. 291-299; Klien N (2004) Internet Governance: Perspectives from Cambodia in MacLean D (ed) Internet Governance: A Grand Collaboration. New York: UN ICT Task Force, pp. 227-237. Excerpts available at http://books.google.ro/ books?id=pEFAypES4t0 C&printsec=frontcover&hl=ro#v=onepage&q&f=fal se [accessed 25 January 2012].

22 ICANN (2005) Principles for the Delegation and Administration of Country Code Top-Level Domains. Available at http://archive.icann.org/en/ committees/gac/gac-cctldprinciples-23feb00.htm [accessed 3 March 2012].

23 The list of root zone servers, their nodes and positions, and managing organisations is available at http://www.root-servers.org/ [accessed 24 January 2012]

24 ISC, Inc. (2003) Hierarchical Anycast for Global Distribution. Available at http://ftp.isc. org/isc/pubs/tn/isc-tn-2003-1.html [accessed 24 January 2012].

25 ICANN CEO talks about new affirmation of commitments. Available at http://www. icann.org/en/news/announcements/announcement-30sep09-en. htm [accessed 11 April 2012].

26 For an overview of the new IANA contract see Weinberger K (2011) A full guide to the new IANA contract. Available at http://news.dot-nxt. com/2011/11/17/full-guide-iana-contract [accessed 30 January 2012].

27 US officials counter that the Internet is too valuable to tinker with or place under an international body like the UN: 'What's at risk is the bureaucratisation of the Internet and innovation', said Michael Gallagher, the Department of Commerce official who administered the government's tie to ICANN. Mr Gallagher and other backers of ICANN also pointed out that the

countries loudest in demanding more international input – China, Libya, Syria, Cuba – have non-democratic governments. Allowing these nations to influence how the Internet works could hinder the freedom of speech, they said. (Source: Rhoads C (2006) Endangered Domain: In Threat to Internet's Clout, Some Are Starting Alternatives. The Wall Street Journal, 19 January 2006; p. A1).

28 Bertola V (no date) Oversight and multiple root server systems. Available at http://www. wgig.org/docs/book/Vittorio_Bertola.html [accessed 11 April 2012].

29 The new signal transmission technologies - both for wireless (like LTE) and optical cables (like DWDM) - promise to solve the "bandwidth exhaust" problem with much greater bandwidth specifications (up to terabits per second). The demand-supply run, however, is perpetual.

30 The Economist (2009) America insists on net neutrality: The rights of bits. 24 September. Available at http://www.economist.com/node/14517422 [accessed 12 October 2012].

31 The sender pays principle follows the traditional economic model of the telephone network, where the party making the call pays for it. Applying this model to the Internet, the party that sends the traffic (provides the content or service) would pay for its delivery to consumers. As result, the cost of network traffic would be largely covered by OTT service provides and the telecomm operators would thereby take a share of their income.

32 Radunovic V (2012) Net neutrality debate goes to the ITU WCIT. Diplo Blog. Available at http://www.diplomacy.edu/blog/net-neutrality-debate-goes-itu-wcit [accessed 11 October 2012].

33 The bandwidth (bit rate) agreed to in a contract with the ISP is, in fact, only the maximum available rather than a guaranteed effective speed.

34 Full text of a Verizon and Google Legislative Framework Proposal for an Open Internet is available at http://docs.google.com/a/diplomacy.edu/viewer?url=http://www.google. com/googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf

35 The case had several turnovers. For more information on the case background, see Broache A (2008) FCC wants to know: Is degrading P2P traffic 'reasonable'? Cnet News Blog. Available at http://news.cnet.com/8301-10784_3-9850611-7.html?tag=mncol;txt [accessed 12 October 2012].

36 The most recent update was the decision of the court against the previous FCC ruling. Kang C (2010) Court rules for Comcast over FCC in 'net neutrality' case. The Washington Post, 7 April. Available at http://www.washingtonpost.com/wp-dyn/content/ article/2010/04/06/AR2010040600742.html [accessed 12 October 2012].

37 Save the Internet is particularly active in advocating network neutrality as preserving the free and open Internet. Available at http://www.savetheinternet.com/ [accessed 12 October 2012].

38 The Internet Governance Caucus (IGC) was originally created by individual and organisational civil society actors who came together in the

context of the World Summit on the Information Society (WSIS) to promote global public interest objectives in Internet governance policy making. Available at http://www.igcaucus.org/ [accessed 12 October 2012].
39 John Herrman illustrates the package offers often used by network neutrality proponents. Available at http://gizmodo.com/5391712/net-neutrality-worst-case [accessed 12 October 2012].
40 La Quadrature du Net, an advocacy group that promotes the rights and freedoms of citizens on the Internet, states within its Open Letter to the European Parliament on Network Neutrality: everyone around the globe has access to the same Internet, and even the smallest entrepreneurs are on equal footing with the leading global enterprises. Available at http://www.laquadrature.net/en/we-must-protect-net-neutrality-in-europe-open-letter-to-the-european-parliament# [accessed 12 October 2012].
41 CNet (2010) Report: Google, Verizon reach Net neutrality deal. Available at http://news.cnet. com/8301-31021_3-20012703-260.html?tag=mncol;mlt_related [accessed 12 October 2012].
42 CNet (2012) European ISPs defend U.N. Internet tax. Available at http://news.cnet. com/8301-13578_3-57496581-38/european-isps-defend-u.n-internet-tax/ [accessed 12 October 2012].
43 Those elements that are still controversial and to be negotiated about in future are in square brackets.
44 Radunovic V (2012) Network Neutrality in law – a step forwards or a step backwards? Diplo Blog. Available at http://www.diplomacy.edu/blog/network-neutrality-law- %E2%80%93-step-forwards-or-step-backwards [accessed 12 October 2012].
45 FCC (2005) Policy statement. Available at http://www.publicknowledge.org/pdf/FCC- 05-151A1.pdf [accessed 12 October 2012].
46 Ministry of Internal Affairs and Communications, Japan (2007) Report on Network Neutrality. Available at http:// www.soumu.go.jp/main_sosiki/joho_tsusin/eng/ pdf/070900_1.pdf [accessed 12 October 2012].
47 PTS (2009) Open Networks and Services. Available at http://www.pts.se/en-gb/ Documents/Reports/Internet/2009/Open-Networks-and-Services---PTS-ER-200932/ [accessed 12 October 2012].
48 Kroes N (2010) Net neutrality in Europe. Speech given by Vice President of the European Commission Commissioner for the Digital Agenda. Available at http://europa.eu/rapid/ pressReleasesAction.do?reference=SPEECH/10/153&format=HTML&aged=0&lang uage=EN&guiLanguage=en [accessed 12 October 2012].
49 Iljitsch van Beijnum (2012) Netherlands becomes world's second "net neutrality" country. Ars Technica. Available at http://arstechnica.com/tech-policy/2012/05/netherlands-becomes-worlds-second-net-neutrality-country/ [accessed 12 October 2012].
50 NPT (2009) Net neutrality: Guidelines for Internet neutrality. Available at http://www. npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf [accessed 12 October 2012].

51 Anderson N (2009) Norway gets net neutrality—voluntary, but broadly supported. Ars Technica. Available at http://arstechnica.com/tech-policy/news/2009/02/norway-gets-voluntary-net-neutrality.ars [accessed 12 October 2012].
52 TechnoLlama (2012) Chile enforces net neutrality for the first time, sort of. Available at http:// www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of [accessed 12 October 2012].
53 Integral text of the 2010 Declaration of the Committee of Ministers on network neutrality of Council of Europe is available at https://wcd.coe.int/ViewDoc.jsp?id=1678287 [accessed 12 October 2012].
54 ISOC considers the concept of network neutrality as rather ill-defined, and instead discusses the continued open inter-networking. Available at http://www.isoc.org/internet/issues/ openinternet.shtml. Its 16 May 2010 Public consultation on Net Neutrality states: Rather than focusing simply on the range of possible Network Neutrality definitions, the Internet Society believes it is more appropriate to concentrate more broadly on the imperative of preserving the open, user-centric Internet model that has been so successful to date. Available at http://www.isoc.org/ regions/europe/docs/netneutrality_20100516_en.pdf [accessed 12 October 2012].
55 TACD (no date) TACD calls for Net Neutrality. Available at http://tacd.org/index. php?option=com_content&task=view&id=162&Itemid=43 [accessed 12 October 2012].
56 Radunovic V (2012) Can free choice hurt open Internet markets? Diplo Blog. Available at http://www.diplomacy.edu/blog/can-free-choice-hurt-open-internet-markets [accessed 12 October 2012].
57 Chetan Sharma lists some interesting opportunities for cooperation between OTT and mobile operators, like analysing real-time network conditions, sharing user behaviour info, location and presence (within limits of privacy regulations), or third-party services billing through mobile subscription: http://synergy.syniverse.com/2012/05/mobile-operators-and-otts-building-a-win-win-partnership/ [accessed 12 October 2012].
58 'The Court of Appeal of The Hague ruled against the Church of Scientology in its copyright infringement suit against a Dutch writer and her ISP, XS4ALL. The writer, formerly a practicing Scientologist, posted to a website parts of confidential church documents, and the church sued under the Dutch Copyright Act of 1912. In 1999, the District Court ruled in favour of the defendants, citing freedom of speech concerns. However, that court also ruled that ISPs should be held liable for posted materials that might violate existing copyrights. The Court of Appeal affirmed the first ruling, but reversed the second, holding that ISPs were not liable for posted materials.' For more information consult Gelman L (2003) Church of Scientology Loses Copyright Infringement Case in Dutch Court. Available at http://cyberlaw. stanford.edu/packets001638.shtml [accessed 15 March 2012].
59 For more information on this case see Electronic Privacy Information Center (2004) RIAA vs Verizon. Available at http://epic.org/privacy/copyright/

verizon/ [accessed 15 March 2012].
60 The Supreme Court of Canada rejected the argument of the Society of Composers, Authors and Music Publishers of Canada that Canadian ISPs should pay royalties because some of their customers download copyrighted works (SOCAN vs CAIP). More information available at http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html [accessed 15 March 2012].
61 'SABAM (the Belgian collective society - Société belge des auteurs, compositeurs et éditeurs) wanted the ISP Scarlet to install a generalised filtering system for all incoming and outgoing electronic communications passing through its services and to block potentially unlawful communications. In First Instance, while refusing the liability of the ISP, the Brussels Court concluded that the SABAM's claim was legitimate and that a filtering system had to be deployed. Scarlet appealed and the case was referred to the Court of Justice of the European Union. In its decision, the Court of Justice ruled that a filtering and blocking system for all its customers for an unlimited period, in abstracto and as preventive measure, violates fundamental rights, more particularly the right to privacy, freedom of communication and freedom of information. In addition, it breaches the freedom of ISPs to conduct business.' For more information, see Scarlet v SABAM: a win for fundamental rights and Internet freedoms EDRi-gram newsletter No 9.23, 30 November 2011. Available at http://www.edri.org/edrigram/number9.23/scarlet-sabam-win-fundamental-rights [accessed 15 March 2012].
62 Williams F (2006) ISPs should be liable for spam, says UN report, Financial Times. Available at http://www.ft.com/cms/s/0/09b837c0-ae02-11da-8ffb-0000779e2340. html#axzz1I2VhnlN0 [accessed 30 January 2012].
63 Shannon V (2006) The end user: Junk payout in spam case - Technology - International Herald Tribune. Available at http://www.nytimes.com/2006/04/12/technology/12iht- PTEND13.1523942.html [accessed 15 March 2012].
64 In computer networking, peering is a voluntary interconnection of administratively separate Internet networks for the purpose of exchanging traffic between the customers of each network. The pure definition of peering is settlement-free or 'sender keeps all', meaning that neither party pays the other for the exchanged traffic; instead, each derives revenue from its own customers. Peering requires physical interconnection of the networks, an exchange of routing information through the Border Gateway Protocol (BGP) routing protocol and is often accompanied by peering agreements of varying formality, from 'handshake' to thick contracts. (Source: Wikipedia)
65 Tier 2 Internet Bandwidth Providers are usually called ICP (Internet connection points) or Internet gateways.
66 Two related cases were mentioned in Spaink and Hardy (2002) Freedom of the internet, our new challenge. Available at http://www.spaink.net/english/osce_internetfreedom. html [accessed 15 March 2012]. In the first case, legal action was launched against a web page with questionable Nazi content hosted by Flashback in Sweden. The courts decided that the page did not

violate Swedish anti-Nazi laws. Nevertheless, one committed anti- Nazi activist mounted a strong campaign against Flashback, thereby putting pressure on Flashback's ISP, Air2Net, and the main backbone operator MCI/WorldCom. Under pressure from this campaign, MCI/WorldCom decided to disconnect Flashback in spite of a lack of any legal basis for doing so. Flashback's attempts to find an alternative provider were unsuccessful, since most of them were also connected through the backbone operated by MCI/WorldCom. The second case took place in the Netherlands. A small Dutch ISP provider, Xtended Internet, was disconnected by its US-based upstream provider under pressure from the Scientology lobby.

67 Andrew Odlyzko views the question of pricing and architecture on the Internet from a historical perspective. Identifying the thread in the pricing policy from the pricing of transportation systems in the ancient world, he links with the current Internet pricing policy. For more information, please consult: Odlyzko A (2004) Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation. Available at http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf [accessed 22 March 2012].

68 Shawn O'Donnell provides an analysis of how 'the Internet dollar flows' explaining where the consumer's ISP dollar goes. See O'Donnell (2002) An Economic Map of the Internet. Center of eBusiness @MIT, Paper 162, September 2002. Available at http://ebusiness.mit. edu/research/papers/2002.09_O%27Donnell_An%20Economic%20Map%20of%20the%20Internet_162.pdf [accessed 22 March 2012].

69 Thuy T, Nguyen T and Armitage GJ (2005) Evaluating Internet Pricing Schemes: A Three- Dimensional Visual Model. ETRI Journal 27(1) pp. 64-74. Available at http://etrij.etri. re.kr/Cyber/BrowseAbstract.jsp?vol=27&pg=64 [accessed 22 March 2012].

70 Hayel Y, Maille P, Tuffin B (2005) Modelling and analysis of Internet Pricing: introduction and challenges In Proceedings of the International Symposium on Applied Stochastic Models and Data Analysis (ASMDA), Brest, France. Available at http://conferences.telecom-bretagne.eu/asmda2005/IMG/pdf/proceedings/1389.pdf [accessed 22 March 2012]

71 Huston G (2005) Where's the Money? - Internet Interconnection and Financial Settlements. The ISP Column. Available at http://www.potaroo.net/ispcol/2005-01/interconn.pdf [accessed 30 January 2012].

72 Techtangerine (no date) Ten reasons why cloud computing is a bad idea. Available at http://www.techtangerine.com/2009/06/02/ten-reasons-why-cloud-computing-is-a-bad-idea/ [accessed 11 April 2012].

73 ACLU White paper (ND) No competition: How monopoly control of the broadband Internet threatens free speech. ACLU: New York, NY, USA. Available at http://www.aclu.org/files/ FilesPDFs/ACF72A9.pdf [accessed 2 February 2012].

74 Global Cybersecurity Agenda. Available at http://www.itu.int/osg/csd/cybersecurity/ gca/ [accessed 11 April 2012].

75 Council of Europe (2001) Convention on Cybercrime. Available at http://

conventions. coe.int/Treaty/en/Treaties/Html/185.htm [accessed 11 April 2012].
76 IWAR(2000) Proposal for an international convention on cyber crime. Available at http://www. iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm [accessed 11 April 2012].
77 DNSSEC explained. Available at http://everything.explained.at/DNSSEC/ [accessed 11 April 2012].
78 For an overview of current status and challenges in DNSSEC deployment see Marsan C (2012) Will 2012 be the dawn of DNSSEC?, 18 January 2012 Networkworld. Available at http://www.networkworld.com/news/2012/011812-dnssec-outlook-255033. html?page=1 [accessed 20 March 2012].
79 The Wassenaar Arrangement. Available at http://www.wassenaar.org/ [accessed 11 April 2012].
80 The Clipper approach was proposed by the US government back in 1993. At its core was the use of a Clipper chip which was supposed to be used in all telephones and other voice communication tools. The Clipper chip had a 'back door' which could be used by governments for lawful surveillance. After strong opposition from human rights activists and the general public, the US government dropped this proposal in 1995. See: Denning D (1995) The case for clipper. MIT Technology Review. MIT: Cambridge, MA, USA. Available at http://encryption_policies.tripod.com/us/denning_0795_clipper.htm [accessed 2 February 2012].
81 More references to Can-Spam are available at the Bureau of Consumer Protection (2009) The CAN-SPAM Act: A Compliance Guide for Business. Available at http://www.ftc.gov/bcp/ edu/pubs/business/ecommerce/bus61. shtm [accessed 2 March 2012].
82 The Contact Network of Spam Enforcement Authorities (CNSA) was established in February 2005 by 13 EU countries (France, Austria, Belgium, Cyprus, the Czech Republic, Denmark, Greece, Ireland, Italy, Lithuania, Malta, the United Kingdom, and Spain). It aims to promote both cooperation among these states and coordination with entities outside the EU, such as the OECD and the ITU.
83 European Commission, Information Society (2010) Unsolicited communication: fighting spam. Available at http://ec.europa.eu/information_society/policy/ecomm/todays_ framework/privacy_protection/spam/index_en.htm [accessed 2 March 2012].
84 As quoted in Johnsson O (2007) Methods to combat SPAM. Available at http://home. swipnet.se/Johnson_Consulting/images/spam1.htm [accessed 20 March 2012].
85 BBC NEWS (2004) European anti-spam laws lack bite. 28 April. Available at http://news. bbc.co.uk/2/hi/technology/3666585.stm [accessed 20 March 2012].
86 For more information about ITU activities related to combating spam see ITU (no date) ITU Activities on Countering Spam. Available at http://www.itu.int/osg/spu/spam/ [accessed 20 March 2012].

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 նկատմամբ1: 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 ՏՀՁԿ 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:

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 ժամանակաշրջանում, 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: Օրինակ՝ Wikipedia միությունը ղեկավարվում է սոցիալ նորմերի միջոցով, որոնք կարգավորում են՝ ինչպես են Wikipedia-ի հոդվածները խմբագրվում և ինչպես են վերջիններիս շուրջ կոնֆլկտներ տարածվում:

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 կարո՞ղ են, արդյոք, լիազորված իրավական ինստիտուտների փոխարեն որոշումներ ընդունել: Մատակարարներն արդյոք կարո՞ղ 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:

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, ԵԽ-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 են3: «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 օրինակարգեր5: 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 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 ինչպե՞ս «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» առաջացմանը9:

Դատական գործերից ամենաակնառուն և շատ հաճախ հիշատակվողներից մեկը, որը լուսաբանում է իրավասության հիմնախնդիրը, 2001 թ. Ֆրանսիայում քննարկված Yahoo!-ի գործն է10: Այդ գործը հերթական անգամ ընդգծեց բազմաքանակ իրավասության հիմնախնդրի կարևորությունը11: 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:

Ազգային օրենքների ներդաշնակություն

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 պոռնոգրական 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 իրականում12: 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:
Աղյուսակ 1-ում ներկայացված է ավանդական դատական համակարգի և միջնորդ դատարանի տարբերությունները.

Աղյուսակ 1. ավանդական դատական համակարգի և միջնորդ դատարանի հիմնական տարբերությունները.

Տարրեր	Դատական համակարգ	Միջնորդ դատարան
Կազմակերպություն	Կարգավորվում է օրենքով/ պայմանագրերով- մշտական	Կարգավորվում է կողմերի միջոցով- ժամանակավոր Կարգավորվում է կոնվենցիաներով- մշտական
Կիրառելի օրենք	Դատարանի օրենք(դատավորն է որոշում կիրառվող օրենքը)	Կողմերը կարող են ընտրել օրենքը, եթե ոչ, ապա պայմանագրում նշված օրենքը, եթե այդպիսին գոյություն չունի, ապա արբիտրաժային մարմնի կողմից կիրառված օրենքը
Պրոցեդուրա	Դատական գործընթացը կարգավորվում է օրենքներով/ պայմանագրերով	Կարգավորվում է կողմերի միջև Կարգավորվում է արբիտրաժային մարմնի կողմից
Իրավասություն/ Վեճերի առարկա	Կարգավորվում է օրենքներով/ պայմանագրերով կապված վեճի առարկայի հետ	Կարգավորվում է կողմերի միջև
Որոշում	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 պայմանագրով13: 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 գործիքներով14: 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 ընթացակարգ15: Սկսած UDRP-ի ներքո իր աշխատանքի սկզբից 1999թ.-ի դեկտեմբերին՝ WIPO միջնորդ դատարանը և Միջնորդության կենտրոնը վարել են ավելի քան 22500 գործ, և նոր gTLD-ի ներմուծման հետ նոր մարտահրավերներ են սպասվում:

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:

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 արտոնագրերին16:

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: Զարմանալի 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: Վերջերս ազգային և միջազգային մակարդակով մի քանի կանոններ են ընդունվել՝ նպատակ ունենալով ուժեղացնել վերահսկումը՝ ստիպելով Համացանցի միջնորդներին ֆիլտրել հեղինակային իրավունքով պաշտպանված բովանդակությունը: Բուռն քննարկումներից հետո 2009թ.-ին Ֆրանսիան ընդունեց HADOPI օրենքը, որը ներկայացնում էր այսպես կոչված երեք հարվածանի գործընթաց հեղինակային իրավունքների առցանց հանցագործների դեմ, որը կարող էր կասեցնել բաժանորդի հասանելությունը Համացանցին: Ապա 2011թ.-ին ԱՄՆ-ում երկու օրինագիծ առաջարկվեց. Առցանց ծովահենության ակտ(SOPA) և IP-ի պաշտպանության ակտ (PIPA), որն առաջարկում էր նոր միջոցներ առցանց ծովահենության դեմ պայքարելու հարցում՝ ներառյալ մուտքի արգելափակում խախտում իրականացված կայք կամ փնտրման արգելում նման կայքերին հղվելու համար: Միջազգային մակարդակով հաստատված միջազգային կառույցների հենքերից դուրս քննարկվեց Հակակեղծարարական առևտրի համաձայնագիրը(ACTA). այն անդրադառնում է IPR-ի խախ-տումներին այնպիսի եղանակով, որը կարող է հնարավորություն ստեղծել մասնավոր (ընկերություններ) հարկադրական և հսկողության գործողությունների համար: Կարգավորման այս գործողությունները խստորեն քննադատվեցին գիտական և քաղաքացիական խմբերի կողմից՝ հիմնվելով մարդու իրավունքների և ազատությունների վրա: Անատական Համացանցային օգտագործողներ միացան առցանց և ցանցից դուրս բողոքների:

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.

- «Տրոյան ձի» 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 (ՄՍՀԿ 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

Հեղինակային 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 ՄՍՀԿ 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 «բրեխիղճ 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՝ հիմնված Բեռնի և Փարիզի պայմանագրերի վրա: Մեկ այլ, դեռևս նոր կազմավորվող կարգ է համակարգում Առեւտրի համաշխարհային կազմակերպությունը (ԱՀԿ) և հիմնվում է մտավոր սեփականության իրավունքների առևտրային տեսանկյունների մասին համաձայնագրի (TRIPS) վրա: Միջազգային մակարդակով մտավոր սեփականության հարցերի համակարգումը ՄՍՀԿ-ից փոխանցվել է ԱՀԿ-ին՝ ՄՍ-ի պաշտպանությունն 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 խուսավարումների 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:

Հեղինակային իրավունքը խախտելու համար պատասխանատվություն

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: ԱՄՆ-ի DMCA և ԵՄ-ի դիրեկտիվների մոտեցումն ազատում է պրովայդերներին օգտոգործողների տեղեկատվության փոխանցման և պահպանման պատասխանատվությունից և պահանջում էր, որ վերջիններս գործեն «Նկատիր և գրանցիր» կարգին համաձայն: Այս լուծումը պրովայդերների համար որոշակի հարմարավետություն է ապահովում, քանի որ վերջիններս ապահովագրվում են օրենսդրական պատժամիջոցներից: Մյուս կողմից, պրովայդերները պոտենցիալ կերպով տեղափոխվում են դատավոր-ների տեսադաշտ և միայն մասնակիորեն են լուծում խնդիրը, քանի որ մրցունակ բովանդակությունները կարող են նաև տեղադրված լինել այլ կայքերում, որը սպասարկում է այլ պրովայդեր: Համացանցում հեղինակային իրավունքի ապագային մասնակիորեն համապատասխան գործ է Grokster-ի և StreamCast-ի գործը. երկու կազմակերպություններ, որոնք իրականացնում են P2P ֆայլ բաշխող ծրագրային ապահովում: Հետևելով DMCA-ի դրույթներին՝ Ամերիկայի ձայնագրման արդյունաբերության ասոցիացիան (RIAA) խնդրեց այս երկու կազմակերպություններին դադարեցնել ֆայլ բաշխող տեխնոլոգիաների զարգացումը, քանի որ վերջիններս նպաստում են հեղինակային իրավունքի խախտ-մանը: Սկզբում, ԱՄՆ-ի դատարանները ողջամիտ հանգամանքների ներքո որոշեցին պատասխանատ-վության չենթակել Grokster-ի և StreamCast-ի նման կազմակերպություններին: Այնուամենայնիվ, 2005թ.-ի հունիսին ԱՄՆ-ի Գերագույն դատարանը որոշեց, որ հե՛նց ծրագրային ապահովման մշակողներն են պատասխանատու հեղինակային իրավունքների հնարավոր չարաշահման համար: Էլեկտրոնային սահմանային հիմնադրամը (EFF) հռչակեց այս գործը որպես նախադեպ ընդդեմ անհատների հայցերի ալիք, և ISP-ի նկատմամբ գործերի քանակը մինչև 2008թ.-ը դարձավ 30 000-ի: Չնայած RIAA-ն դադարեցրեց իր դատական արշավը՝ հեղինակային իրավունքների խախտումները շարունակում են մնալ ուշադրության կենտրոնում և տեխնոլոգիաների զարգացման տեմպին համապատասխան դիվերսիֆիկացվում է:

Արտոնագրեր

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 կազմակերպությունը17: 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 է18: 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 մասում19:

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 համարվում20:

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 պոռնոգրաֆիան 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 ազատությունը21: 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

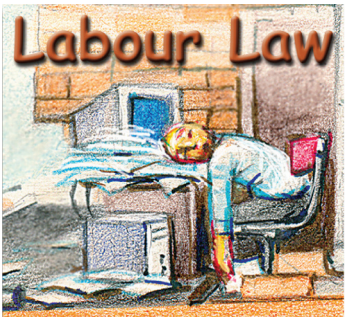
Հաճախ են խոսում այն մասին, որ համացանցը փոխում է աշխատանքային գործունեության բնույթը: Այս երևույթը, թեև մանրամասն քննարկում է պահանջում, սակայն անմիջականորեն համացանցի կառավարման համար մեծ կարևորություն ունեն հետևյալ տեսակետները.

- 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:

Մասնավոր կյանքի գաղտնիքը և տվյալների պահպանումը21

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 անքակտելի 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 սեկտոր22:

Հարցեր

Անհատներ և պետություններ

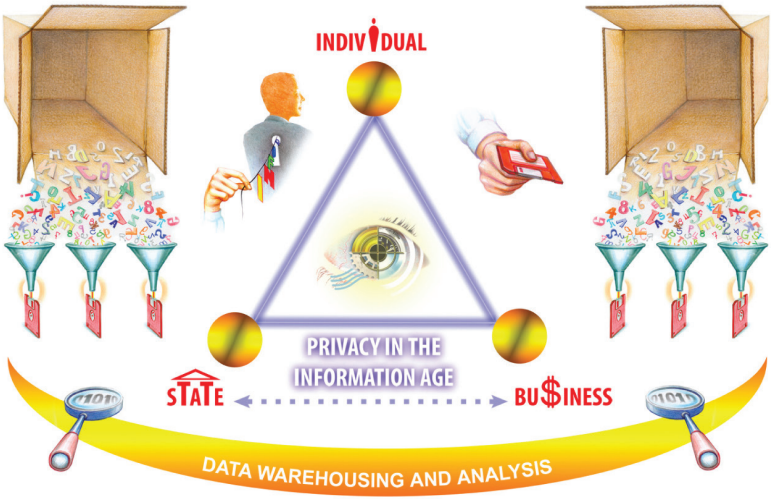
Իշխանական մարմինների համար տեղեկատվությունը միշտ եղել է տարածքներն ու բնակչությանը վերահսկելու կարևորագույն գործիքը: Կառավարությունները հավաքում են անձնական մեծածավալ տեղեկություններ (ծնունդների եւ ամուսնությունների գրանցման, անձնագրերի համարների, քվեարկությունների, դատվածության մասին տվյալներ, հարկային 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 իրավունքը23: Հանցանշաններ հավաքելու նպատակով օրինականորեն խափանելու հայեցակարգը ընդգրկված է նաև կիբեռհանցագործության մասին Եվրախորհրդի պայմանագրում (էջ՝ 20 և21):
Մասնավոր կյանքի գաղտնիության պահպանումը. անհատները 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, 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. անհատներ և անհատներ

Մասնավոր կյանքի գաղտնիքի պահպանման վերջին տեսակետը 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 պայմանագիրը: 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 սահմաներից 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» փաստաթուղթը, բժշկական տեղեկատվության գաղտնիությունն ապահովելու է առողջապահության ու սոցիալական ապահովության մասին վերջերս առաջարկված օրենքների փաթեթը:

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): Հաշվի առնելով Եվրամիության համար գաղտնիության և տվյալների պահպանման հարցերի կարևորությունը, եվրոպական քաղաքագետները, հավանաբար, պետք է մի նոր բանով փոխարինեն այլևս չաշխատող «հուսալի հանգրվանի» մասին համաձայնգիրը:

Ծանոթագրություններ

The White House (1997) Framework for Global Electronic Commerce. Available at http:// clinton4.nara.gov/WH/New/Commerce/ [accessed 11 April 2012].
2 WTO (1998) Work programme on electronic commerce. Available at http://www.wto.org/ english/tratop_e/ecom_e/wkprog_e.htm [accessed 25 February 2012].
3 European Union [EU] (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=CELEX:32000L0031:EN:NOT [accessed 24 February 2012].
4 WTO (no date) GATT and the Goods Council. Available at http://www.wto.org/ english/tratop_e/gatt_e/gatt_e.htm [accessed 11 April 2012].
5 WTO (1994) Agreement on Trade-related Aspects of Intellectual Property Rights. Available at http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm [accessed 11 April 2012].
6 This section of the WTO website focuses on e-commerce. Available at http://www.wto. org/english/tratop_e/ecom_e/ecom_e.htm [accessed 25 February 2012].
7 For more information about the USA/Antigua Online Gambling Case, please consult http:// www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm [accessed 25 February 2012].
8 UNCITRAL website. Available at http://www.uncitral.org/uncitral/index.html [accessed 11 April 2012].
9 UNCITRAL (1996) Model Law on Electronic Commerce. Available at http://www. uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html [accessed 11 April 2012].
10 ebXML website. Available at http://www.ebxml.org/ [accessed 11 April 2012].
11 See for example a discussion about the relevance of ebXML standard today here: http:// www.infoq.com/news/2012/01/ebxml [accessed 2 April 2012].
12 UNCTAD (no date) Economic reports. Available at http://archive.unctad.org/ Templates/Page.asp?intItemID=3594&lang=1 [accessed 11 April 2012].
13 International Chamber of Commerce website. Available at http://www.iccwbo.org/ [accessed 11 April 2012].
14 The Global Business Dialogue website. Available at http://www.gbdinc.org/ [accessed 11 April 2012].
15 European Commission (no date) E-commerce directive. Available at http://ec.europa.eu/ internal_market/e-commerce/directive_en.htm [accessed 11 April 2012].

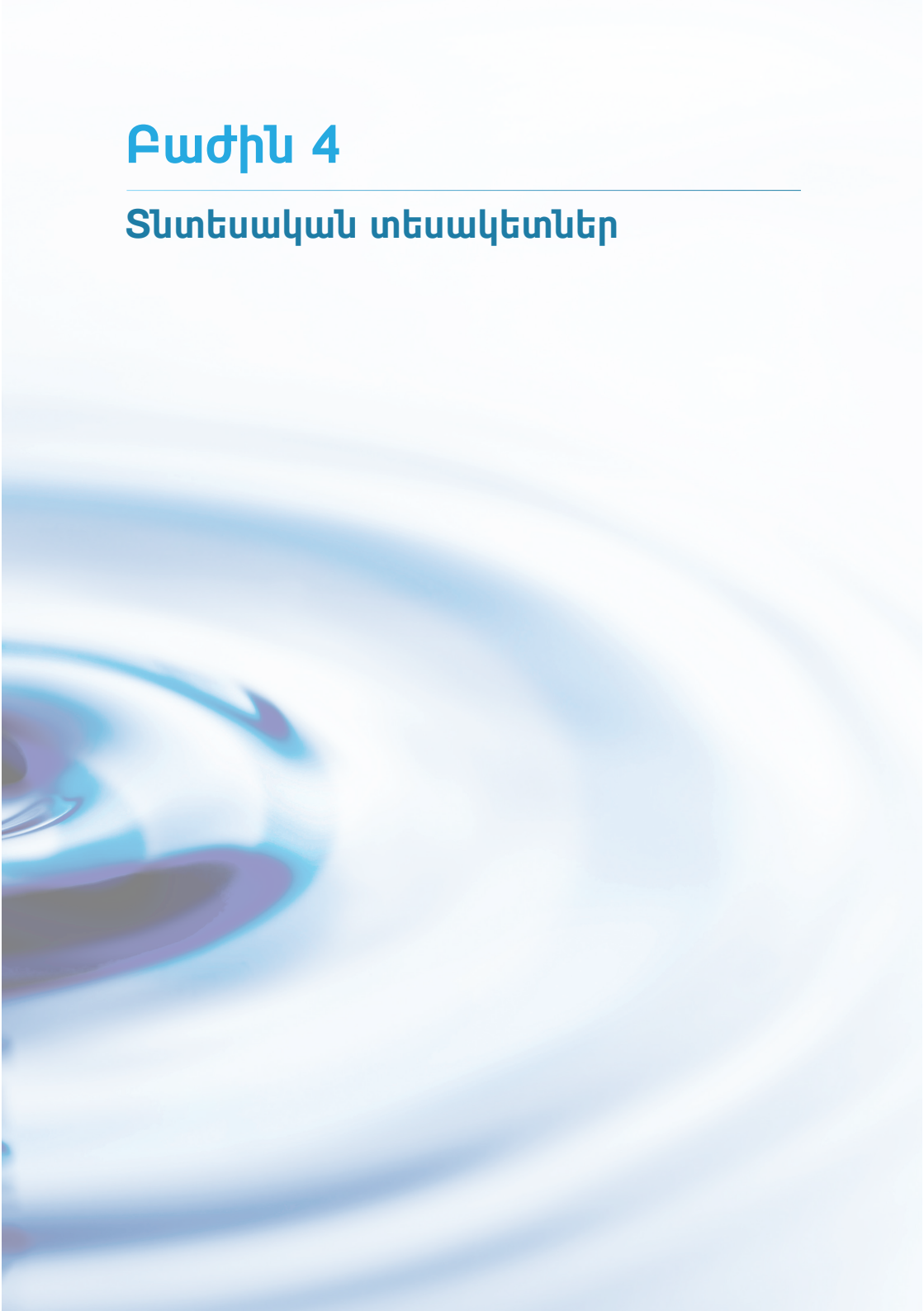
16 APEC (no date) Paperless Trading Individual Action Plan. Available at http://www.apec. org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering- Group/Paperless-Trading-Individual-Action-Plan.aspx [accessed 11 April 2012].
17 OECD (1999) Guidelines for Consumer Protection in the Context of Economic Commerce. Available at http://www.oecd.org/document/51/0,3746, en_21571361_43348316_1824435_1_1_1_1,00.html [accessed 11 April 2012]
18 OECD (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices. Available at http://www.oecd.org/ document/50/0,3746, en_2649_34267_2514994_1_1_1_1,00.html [accessed 11 April 2012].
19 Better Business Bureaus website. Available at http://www.bbb.org/us/ cbbb/ [accessed 11 April 2012].
20 Europe (no date) Brussels I. Available at http://europa.eu/legislation_ summaries/ justice_freedom_security/judicial_cooperation_in_civil_matters/ l33054_en.htm [accessed 11 April 2012].
21 The Gallup Organisation (2011) Consumer attitudes towards cross-border trade and consumer protection. Analytical Report. Flash Eurobarometer. Available at http://ec.europa.eu/consumers/ strategy/docs/ consumer_eurobarometer_2011_en.pdf [accessed 25 February 2012].
22 UNCITRAL (1980) UN CISG. Available at http://www.uncitral.org/uncitral/ uncitral_ texts/sale_goods/1980CISG.html [accessed 11 April 2012].
23 Maastricht Economic Research Institute on Innovation and Technology (MERIT) (1999). Cybertax Available at http://www.merit.unimaas.nl/cybertax/ [accessed 25 February 2012].
24 For a discussion on various aspects of taxation policy and the Internet, please consult:
• Cockfield AJ (2001) Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation, 85 Minn. L. Rev. 1171, 1235-1236.
• Morse EA (1997) State Taxation of Internet Commerce: Something New under the Sun? 30 Creighton L. Rev. 1113, 1124-1227.
• Williams WR (2001) The Role of Caesar in the Next Millennium? Taxation of E-Commerce: An Overview and Analysis, 27 Wm Mitchell L. Rev. 1703, 1707.
25 Internet Tax Freedom Act. Available at http://legacy.gseis.ucla.edu/iclp/ itfa.htm [accessed 11 April 2012].
26 Mazerov M (2007) Making the 'Internet Tax Freedom Act' Permanent Could Lead to a Substantial Revenue Loss for States and Localities. Available at http://www.cbpp.org/7-11- 07sfp.htm [accessed 26 February 2012].
27 The Ottawa Taxation Principles are: Neutrality, Efficiency, Certainty and simplicity, Effectiveness and fairness, Flexibility. See OECD (2003) Implementation of the Ottawa Taxation Framework Conditions. The 2003 Report. Available at http://www.oecd.org/ dataoecd/45/19/20499630.pdf [accessed 4 April 2012].
28 For a more detailed explanation of these three approaches, please

consult: ILPF (no date) Survey of International Electronic and Digital Signature Initiatives. Available at http://www. ilpf.org/groups/survey.htm#IB [accessed 27 February 2012].
29 European Commission (1999) Directive on Electronic Signatures. Available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc =31999L0093&model=guichett [accessed 11 April 2012].
30 European Commission (2006) Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures Available at http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF [accessed 27 February 2012].
31 UNCITRAL (2001) Model Law on Electronic Signatures. Available at http://www. uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html [accessed 11 April 2012].
32 More information on GUIDEC elaboration can be found on the ICC dedicated webpage. Available at http://www.iccwbo.org/policy/ebitt/id2340/index.html [accessed 27 February 2012].
33 Longmuir G (2000) Privacy and Digital Authentication Available at http://caligula.anu. edu.au/~gavin/ResearchPaper.htm [accessed 27 February 2012]. This paper focuses on the personal, community, and governmental aspects of the need for authentication in a digital world.
34 As reported in Olson T (2012) Higher costs, new laws mean no more free rides on some bank services, accounts. Pittsburgh Tribune-Review, April 1. Available at http://www. pittsburghlive.com/x/pittsburghtrib/business/s_789300.html [accessed 1 April 2012].
35 Nsouli S and Schaechter A (2002) Challenges of the 'E-Banking Revolution', Finance and Development 39(3). Available at http://www.imf.org/external/pubs/ft/fandd/2002/09/ nsouli.htm [accessed 28 February 2012].
36 Basel Committee on Banking Supervision (1998) Risk Management for Electronic Banking and Electronic Money Activities. Basel March 1998 Available at http://www.bis.org/publ/ bcbs35.pdf [accessed 28 February 2012].
37 appsworldblog (2011) 5 Reasons why you need to be ready for Mobile Payments. August 10. Available at http://www.apps-world.net/blog/2011/08/media-partners/5-reasons-why-you-need-to-be-ready-for-mobile-payments/ [accessed 5 April 2012].
38 This article provides an introduction to online banking and a survey of the advantages and disadvantages in comparison to traditional banking. Available at http://www.bankrate. com/brm/olbstep2.asp [accessed 28 February 2012].
39 Wikipedia (no date) SOXA. Available at http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act [accessed 11 April 2012].
40 For more information, please consult: Jacobs E (no date), Security as a Legal Obligation: About EU Legislation Related to Security and Sarbanes-Oxley in the European Union. Available at http://www.arraydev.com/commerce/JIBC/2005-08/security.htm [accessed 28 February 2012].

41 European Commission (no date) E-money. Available at http://ec.europa.eu/internal_ market/payments/emoney/index_en.htm [accessed 11 April 2012].
42 As quoted in Holland K and Cortese A (1995) The future of money: e-cash could transform the world's financial life. Available at http://www.businessweek.com/1995/24/b3428001.htm [accessed 29 March 2012].
43 For arguments against micro-payments, please consult: Shirky C (2000) The Case against Micropayments. Available at http://www.openp2p.com/pub/a/p2p/2000/12/19/ micropayments.html [accessed 28 February 2012].
44 The Basel Group is based at the Bank for International Settlements. It provides a Survey of Developments in Electronic Money and Internet and Mobile Payments. Available at http:// www.bis.org/publ/cpss62.pdf [accessed 28 February 2012].
45 Richtel M (2002) PayPal and New York in Accord on Gambling. The New York Times, August 22. Available at http://www.nytimes.com/2002/08/22/business/technology-paypal-and-new-york-in-accord-on-gambling.html?src=pm [accessed 29 March 2012].
46 Prater C (2009) What you buy, where you shop may affect your credit. Available at http://www. creditcards.com/credit-card-news/how-shopping-can-affect-credit-1282.php [accessed 29 March 2012].

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 հետևանքներ1: 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 բանավեճը2:
- Վեճերի լուծման մեխանիզմ: Էլեկտրոնային առևտրին անմիջականորեն վերաբերող փայլուն օրինակ է «ԱՄՆ-ն ընդդեմ Անտիգուայի» գործը, որը կապված էր առցանց մոլի խաղերին3: Էլեկտրոնային առևտրի հարցերը, թեև մինչև հիմա մնացել 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:

Ի՞նչ 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 ՄՄՀԿ պայմանագրերը, զարգացած երկրները փորձում էին ընդլայնել TRIPS կիրառման ոլորտը էլեկտրոնային առևտրի և համացանցի մոջոցով, 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 մնում 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:

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 ՏՀԶԿ 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): 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: ԱԽՏՀ-ի ամենից նշանավոր նախաձեռնություններից էր Առանց թղթաբանության գործողությունների անհատական ծրագիրէ, որը նպատակաուղղված էր առանց թղթաբանության միջսահմանային առևտրի համակարգ ստեղծելուն:

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 (1999 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: Նույնիսկ ԵՄ-ի հաստա-տած լայն կարգավորման պարագայում առցանց գնումները տարածաշրջանում մնում են հարաբերականորեն ցածր մակարդակի վրա. 2010թ.-ին ԵՄ-ի քաղքացիների միայն 37%-ն են իրեր գնել առցանց եղանակով և միայն 7%-ն է տեղադրել միջսահմանային պատվերներ, ինչն իր հերթին նշանակում է առցանց խանութների նկատմամբ ցածր վստահություն, հատկապես երբ խոսքը գնում է արտասահմանյան տարրերի մասին:
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:

Ժամանակակից հասարակության հոսք Համցանցի ներխուժմանը զուգընթաց հարկման հարցը դարձավ ուշադրության կենտրոնում: Այն առավել կարևոր դարձավ 2008թ.-ի տնտեսական ճգնաժամի ժամանակ: Շատ կառավարություններ փորձում էին մեծացնել ֆինանսական եկամուտները աճող պետական պարտքը կրճատելու նպատակով: Համացանցում տնտեսական գործունեությունը հարկելը դարձավ ֆինասական եկամուտները մեծացնելու առաջին հնարավոր տարբերակը: Ամենից հաճախակի հարցումներից էր առցանց դրամախաղի սահմանափակումը, որպեսզի վերջ տրվեր հարկային եկամուտների արտահոսքն ավանդական դրամախաղային կենտրոններում: Այլ առաջարկներից էր Համացանցային հասանելիության նկատմամբ հատուկ հարկի կիրառումը:

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:

ՏՀԶԿ-ն և ԵՄ-ն պնդում են հակառակ դիրքորոշումը, այն է՝ հարկման առումով համացանցի համար որևէ բացառություն չպետք է արվի: Օտտավայի ՏՀԶԿ 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 թվային 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»: Ի՞նչ 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 կա:

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 գաղտնիության պահպանումն ու թվայնացված ստորագրությունները

Էլեկտրոնային թվայնացված ստորագրությունները ավելի մեծածավալ հիմնախնդրի՝ համացանցում գաղտնիության ու անձի ինքնության հավաստագրման միջև հավասարակշռության մի մասն է: ԷԹՍ-ն կարևոր տեխնոլոգիաներից ընդամենը մեկն է (բայց ոչ միակը), որ թույլ է տալիս համացանցում հավաստել օգտատիրոջ անձը: Օրինակ՝ որոշ երկրներում, որտեղ ԷԹՍ-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 ԷԹՍ-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 4 դոլար, համացանց-բանկային ձևով կատարելիս արժե ընդամենը 0,17 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

Մոբայլ առևտուր

Էլեկտրոնային վճարումները և էլեկտրոնային փողերը ներկայումս արագ ընթացող փոփոխություններ են տեխնոլոգիայի և սարքերի զարգացմանը զուգընթաց: Բջջային վճարումները արդեն իսկ գերազանցել են պարզ պատվերները հաղորդագրությունների միջոցով, քանի որ բջջային հեռախոսները դարձել են ավելի բարդեցված և «ինտելեկտուալ»՝ թույլատրելով տարբեր ծրագրերի կիրառումը բջջային առևտրում:

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

Աշխարհում բանկային համակարգի փոփոխություններ

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:

Կիբեռանվտանգությունը

Կիբեռանվտանգությունը էլեկտրոնային վճարումների լայնորեն տարածման ճանապարհին հիմնական բարդություններից մեկն է: Համացանցում ինչպե՞ս երաշխավորել ֆինանսական գործողությունների անվտանգությունը: Կիբեռանվտանգութ֊ան 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 World-Com 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:

Վճարման մեթոդների սակավություն

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:

Թվային դրամ

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:

Փոքր գործարքներ

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:

Հարցին միջազգային մակարդակով անդրադառնալը

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:

Հարկադրանքի հղման օրենքը

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:

Գաղտնիություն

Էլեկտրոնային վճարումների համակարգի օգտագործումը յուրաքանչյուր կատարված գործարքի վերաբերյալ հետք է թողնում, ինչը գրանցվում է էլեկտրոնային վճարման գործիքի թողարկողի կողմից (կրեդիտ քարտերի կազմակերպություններ, բանկեր): Թեև այսպիսի գրանցումներ պահպանելն անհրաժեշտ է և վճարման առկայությունը ապացույցելու համար արդարացված, նմանատիպ տվյալների հավաքագրումը կարող է լուրջ վտանգ ստեղծել օգտագործողների գաղտնիության համար, եթե տվյալների հավաքագրումն օգտագործվում է վճարումները և ծախսելու սովորույթները հետևելու կամ հաճախորդներին ապագայում ծառայություն մատուցելու հնարավորությունը գնահատելու համար:

Ծանոթագրություններ

1 The White House (1997) Framework for Global Electronic Commerce. Available at http:// clinton4.nara.gov/WH/New/Commerce/ [accessed 11 April 2012].
2 WTO (1998) Work programme on electronic commerce. Available at http://www.wto.org/ english/tratop_e/ecom_e/wkprog_e.htm [accessed 25 February 2012].
3 European Union [EU] (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=CELEX:32000L0031:EN:NOT [accessed 24 February 2012].
4 WTO (no date) GATT and the Goods Council. Available at http://www.wto.org/ english/tratop_e/gatt_e/gatt_e.htm [accessed 11 April 2012].
5 WTO (1994) Agreement on Trade-related Aspects of Intellectual Property Rights. Available at http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm [accessed 11 April 2012].
6 This section of the WTO website focuses on e-commerce. Available at http://www.wto. org/english/tratop_e/ecom_e/ecom_e.htm [accessed 25 February 2012].
7 For more information about the USA/Antigua Online Gambling Case, please consult http:// www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm [accessed 25 February 2012].
UNCITRAL website. Available at http://www.uncitral.org/uncitral/index.html [accessed 11 April 2012].
9 UNCITRAL (1996) Model Law on Electronic Commerce. Available at http://www. uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html [accessed 11 April 2012].
10 ebXML website. Available at http://www.ebxml.org/ [accessed 11 April 2012].
11 See for example a discussion about the relevance of ebXML standard today here: http:// www.infoq.com/news/2012/01/ebxml [accessed 2 April 2012].
12 UNCTAD (no date) Economic reports. Available at http://archive.unctad.org/ Templates/Page.asp?intItemID=3594&lang=1 [accessed 11 April 2012].
13 International Chamber of Commerce website. Available at http://www.iccwbo.org/ [accessed 11 April 2012].
14 The Global Business Dialogue website. Available at http://www.gbdinc.org/ [accessed 11 April 2012].
15 European Commission (no date) E-commerce directive. Available at http://ec.europa.eu/ internal_market/e-commerce/directive_en.htm [accessed 11 April 2012].

16 APEC (no date) Paperless Trading Individual Action Plan. Available at http://www.apec. org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering- Group/Paperless-Trading-Individual-Action-Plan.aspx [accessed 11 April 2012].
17 OECD (1999) Guidelines for Consumer Protection in the Context of Economic Commerce. Available at http://www.oecd.org/document/51/0,3746, en_21571361_43348316_1824435_1_1_1_1,00.html [accessed 11 April 2012].
18 OECD (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices. Available at http://www.oecd.org/ document/50/0,3746, en_2649_34267_2514994_1_1_1_1,00.html [accessed 11 April 2012].
19 Better Business Bureaus website. Available at http://www.bbb.org/us/ cbbb/ [accessed 11 April 2012].
20 Europe (no date) Brussels I. Available at http://europa.eu/legislation_ summaries/ justice_freedom_security/judicial_cooperation_in_civil_matters/ l33054_en.htm [accessed 11 April 2012].
21 The Gallup Organisation (2011) Consumer attitudes towards cross-border trade and consumer protection. Analytical Report. Flash Eurobarometer. Available at http://ec.europa.eu/consumers/ strategy/docs/ consumer_eurobarometer_2011_en.pdf [accessed 25 February 2012].
22 UNCITRAL (1980) UN CISG. Available at http://www.uncitral.org/uncitral/ uncitral_ texts/sale_goods/1980CISG.html [accessed 11 April 2012].
23 Maastricht Economic Research Institute on Innovation and Technology (MERIT) (1999). Cybertax Available at http://www.merit.unimaas.nl/cybertax/ [accessed 25 February 2012].
24 For a discussion on various aspects of taxation policy and the Internet, please consult:
• Cockfield AJ (2001) Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation, 85 Minn. L. Rev. 1171, 1235-1236.
• Morse EA (1997) State Taxation of Internet Commerce: Something New under the Sun? 30 Creighton L. Rev. 1113, 1124-1227.
• Williams WR (2001) The Role of Caesar in the Next Millennium? Taxation of E-Commerce: An Overview and Analysis, 27 Wm Mitchell L. Rev. 1703, 1707.
25 Internet Tax Freedom Act. Available at http://legacy.gseis.ucla.edu/iclp/ itfa.htm [accessed 11 April 2012].
26 Mazerov M (2007) Making the 'Internet Tax Freedom Act' Permanent Could Lead to a Substantial Revenue Loss for States and Localities. Available at http://www.cbpp.org/7-11- 07sfp.htm [accessed 26 February 2012].
27 The Ottawa Taxation Principles are: Neutrality, Efficiency, Certainty and simplicity, Effectiveness and fairness, Flexibility. See OECD (2003) Implementation of the Ottawa Taxation Framework Conditions. The 2003 Report. Available at http://www.oecd.org/ dataoecd/45/19/20499630.pdf [accessed 4 April 2012].
28 For a more detailed explanation of these three approaches, please

consult: ILPF (no date) Survey of International Electronic and Digital Signature Initiatives. Available at http://www. ilpf.org/groups/survey.htm#IB [accessed 27 February 2012].
29 European Commission (1999) Directive on Electronic Signatures. Available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc =31999L0093&model=guichett [accessed 11 April 2012].
30 European Commission (2006) Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures Available at http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF [accessed 27 February 2012].
31 UNCITRAL (2001) Model Law on Electronic Signatures. Available at http://www. uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html [accessed 11 April 2012].
32 More information on GUIDEC elaboration can be found on the ICC dedicated webpage. Available at http://www.iccwbo.org/policy/ebitt/id2340/index.html [accessed 27 February 2012].
33 Longmuir G (2000) Privacy and Digital Authentication Available at http://caligula.anu. edu.au/~gavin/ResearchPaper.htm [accessed 27 February 2012]. This paper focuses on the personal, community, and governmental aspects of the need for authentication in a digital world.
34 As reported in Olson T (2012) Higher costs, new laws mean no more free rides on some bank services, accounts. Pittsburgh Tribune-Review, April 1. Available at http://www. pittsburghlive.com/x/pittsburghtrib/business/s_789300.html [accessed 1 April 2012].
35 Nsouli S and Schaechter A (2002) Challenges of the 'E-Banking Revolution', Finance and Development 39(3). Available at http://www.imf.org/external/pubs/ft/fandd/2002/09/ nsouli.htm [accessed 28 February 2012].
36 Basel Committee on Banking Supervision (1998) Risk Management for Electronic Banking and Electronic Money Activities. Basel March 1998 Available at http://www.bis.org/publ/ bcbs35.pdf [accessed 28 February 2012].
37 appsworldblog (2011) 5 Reasons why you need to be ready for Mobile Payments. August 10. Available at http://www.apps-world.net/blog/2011/08/media-partners/5-reasons-why-you-need-to-be-ready-for-mobile-payments/ [accessed 5 April 2012].
38 This article provides an introduction to online banking and a survey of the advantages and disadvantages in comparison to traditional banking. Available at http://www.bankrate. com/brm/olbstep2.asp [accessed 28 February 2012].
39 Wikipedia (no date) SOXA. Available at http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act [accessed 11 April 2012].
40 For more information, please consult: Jacobs E (no date), Security as a Legal Obligation: About EU Legislation Related to Security and Sarbanes-Oxley in the European Union. Available at http://www.arraydev.com/commerce/JIBC/2005-08/security.htm [accessed 28 February 2012].

41 European Commission (no date) E-money. Available at http://ec.europa.eu/internal_ market/payments/emoney/index_en.htm [accessed 11 April 2012].
42 As quoted in Holland K and Cortese A (1995) The future of money: e-cash could transform the world's financial life. Available at http://www.businessweek.com/1995/24/b3428001.htm [accessed 29 March 2012].
43 For arguments against micro-payments, please consult: Shirky C (2000) The Case against Micropayments. Available at http://www.openp2p.com/pub/a/p2p/2000/12/19/ micropayments.html [accessed 28 February 2012].
44 The Basel Group is based at the Bank for International Settlements. It provides a Survey of Developments in Electronic Money and Internet and Mobile Payments. Available at http:// www.bis.org/publ/cpss62.pdf [accessed 28 February 2012].
45 Richtel M (2002) PayPal and New York in Accord on Gambling. The New York Times, August 22. Available at http://www.nytimes.com/2002/08/22/business/technology-paypal-and-new-york-in-accord-on-gambling.html?src=pm [accessed 29 March 2012].
46 Prater C (2009) What you buy, where you shop may affect your credit. Available at http://www. creditcards.com/credit-card-news/how-shopping-can-affect-credit-1282.php [accessed 29 March 2012].

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: 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.
- 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:
Այս մտահոգիչ առանցքը շարունակվեց IGF-ի շրջանակներում, որտեղ թեմայի զարգացումն ընդգծվեց 2006թ.-ին Աթենքում առաջին հանդիպման ժամանակ և շարունակվեց սեմինարների, նույնիսկ 2010թ.-ի Վիլնյուսի հիմնական նիստի ժամանակ: Զարգացման հետ կապված հարցերը ամենից հայտնի հարցերի հնգյակում էին, որոնք բարձրացվել էին IGF-ի շարունակականության քննարկման համատեքստում՝ հատկապես զարգացող երկրների մասնակցության մեծացնելով և առաջնահեր-թությունը զարգացմանը տալով: Որպես արդյունք, IDF-ի վեցերերդ հանդիպմանը Նայրոբիում 2011թ.-ին գացումը եղավ խաչվող թեմա և Համացանցի կառավարումը

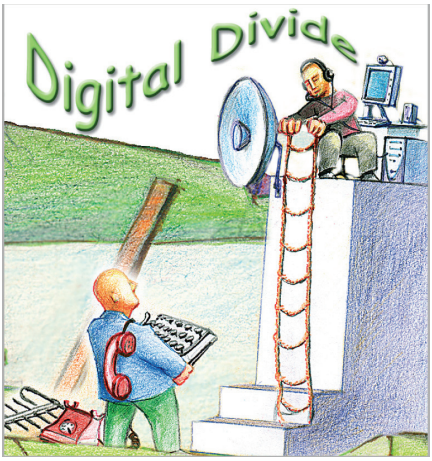
զարգացման համար գողափարն ի հայտ եկավ(IG4D):

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 մեջ» 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») վնաս 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:

Մեծանում 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: Այնուամենայնիվ, թվային բացթողումները գնահատելու չափանիշները ևս փոխվում են և էլ ավելի բարդեցված դառնում, որպեսզի ներառեն իրական զարգացումները: Ներկու գնահատումը հաշվի է առնում այնպիսի բնագավառներ, ինչպիսիք են ՏՀՏ պատրաստվածության և ընդհանուր ՏՀՏ-ի ազդեցությունը հասարակության վրա: Աշխարհի տնտեսական ֆորում(WEF) –ը 2012թ.- իր «Գլոբալ ինֆորմացիոն տեխնոլոգիաների զեկույց 2012» զեկույցում օգտագործեց Ցանցի պատրաստվածության ինդեքսը (NRI)՝ անդրադառնալով Համացանցին արագ հասանելության պատճառներին և հետևանքնե-րին, որը նոր տեսանկյունից էր դիտարկում թվային բաժանման գաղափարը:

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 մնում 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 տարածաշրջանիերում, 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 ձեռնարկել3:

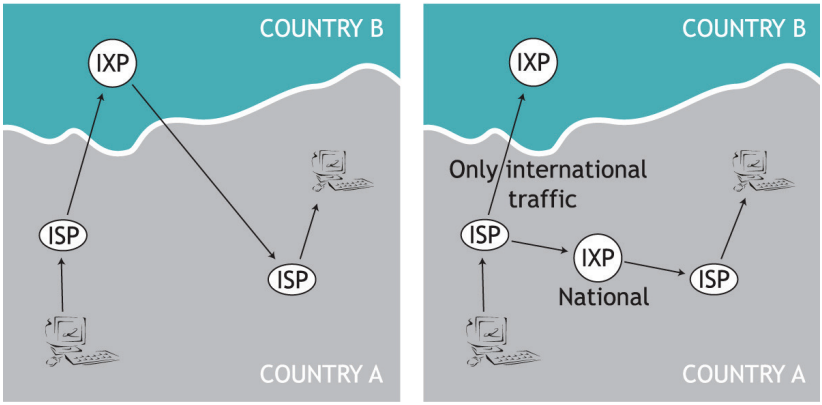
«Թվային խզումը» հաղթահարելու ռազմավարություն

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

Համացանցին հասանելիությունը թվային խզումը հաղթահարելու համար մարտահրավերներից մեկն: 2011թ.-ին Աֆրիկայում Համացանցի ներթափանցվածության աստիճանը 13.5 տոկոս էր կազմում, մինչդեռ Հյուսիսային Ամերիկայում 78.6 տոկոս է, իսկ Եվրոպայում՝ 61.3 տոկոս: Միևնույն ժամանակ սա վերջին տասնամյակում գրանցված ամենաբարձր աճն էր: Գոյություն ունի երկու հիմնական տեսակետ կապված զարգացող երկրներում Համացանցին հասանելիության հետ:



Առաջինը միջազգային Համացանցի հիմքն է, երկրորդը՝ կապը զարգացող երկրներում: Առաջինը գլխավորապես կախված է ստորջրյա օպտիկամարաթելային մալուխներից: Երկար ժամանակ միայն Արևմտյան Աֆրիկայից մինչև Հարավային Աֆրիկա ընկնող հատվածը սպասարկվում էր SAT-3 մալուխով: Ապա Արևելյան Աֆրիկան ևս ստացավ հասանելիություն ստորջրյա մալուխներին. Արևելյան Աֆրիկայի ստորջրյա համակարգը(EASSY) սկսեց գործել 2010թ.-ի հուլիսին: Մի քանի լրացուցիչ ստորջրյա մալուխներ կշահագործվեն մոտակա տարիների ընթացքում: Դա հոզոր թվային օղակ կստեղծի Աֆրիկայի շուրջ, որն էականորեն կբարձրացնի Համացանցի հասանելիությունը ողջ աֆրիկյան մայրցամաքում:
Փոքր հեռավոր կղզիները նմանատիպ դժվարությունների առջև են կանգնած, քանի որ նրանցից շատերը կախված են թանկ արբանյակային կապից: Ջանքեր են տարվում նմանատիպ տարածքներում առավել արդյունավետ լուծումը գտնելու համար: Հնարավոր լուծումներից է համարվում Համացանցի փոխանակման կետերի(IXPs) ներմուծումը, ինչը թույլ կտա տեղական թրաֆիկը պահպանել երկրի մեջ և նվազեցնել միջազգային թողունակության և՛ օգտագործումը, և՛ արժեքը: IXP-ները տեխնիկական սարքավորումներ են, որոնց միջոցով տարբեր պրովայդերներ փոխանակում են Համացանցի թրաֆիկը: Վերջիններս սովորաբար օգտագործվում են Համացանցի թրաֆիկը փոքր շրջանակներում պահպանելու համար, օրինակ՝ քաղաք, տարածաշրջան, երկիր՝ հեռավոր աշխարհագրական տարածքի շուրջ անցան-կալի երթուղավորումից խուսափելով: IXP-ները կարող են նաև կարևոր դեր խաղալ թվային բաժանումը նվազեցնելու հարցում: Այդուհանդերձ, շատ զարգացող երկրներ չունեն IXP-ները, ինչը նշանակում է, որ երկրի ներսում օգտագործողների միջև թրաֆիկը երթուղավորվում է այլ երկրի միջոցով: Սա մեծացնում է տվյալների միջքաղաքային և միջազգային թրաֆիկի ծավալը և Համացանցային ծառայությունների մատակարարման արժեքը: Կան IXP-ները զարգացող երկներում տեղադրելու բազմաթիվ նախաձեռ-նություններ: Դրանցից մեկը, որը զգալի չափով հաջողության է հասել, Աֆրիկայի Համացանցային ծառա-յությունների մատակարարման ասոցիացան է: Այս ասոցիացան պատասխանատու է Աֆրիկայում մի քանի IXP-ներ տեղադրելու

համար:
Կապը զարգացող երկրներում այլ լուրջ խնդիր է: Համացանցի օգտատերերի մեծ մասըկենտրոնացված են խոշոր քաղաքներում: Գյուղական տարածքներում Համացանցին հասանելիություն սովորաբար չի լինում: Այս իրավիճակը սկսեց փոխվել բջջային հեռախոսների և անլար հեռահաղորդակցության աճին զուգընթաց: Անլար հաղորդակցային կապը կարող է օգնել լուծելու վերերկրյա հեռահաղորդակ-ցությունների 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:

Ֆինանսական աջակցություն

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:
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:

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 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 միջոցով5:

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:
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

United Nations General Assembly [UNGA] (2002) Resolution 56/183. World Summit on the Information Society (A/RES/56/183). Available at http://www.itu.int/wsis/docs/ background/resolutions/56_183_unga_2002.pdf [accessed 10 April 2012].
2 UN Millennium Declaration (2000) Available at http://www.un.org/millennium/ declaration/ares552e.htm [accessed 17 October 2012].
3 United Nations (no date) Millennium Development Goals. Available at http://www. un.org/millenniumgoals/ [accessed 17 October 2012].
4 auDA (no date) Continuation of the Internet Governance Forum. Analysis of the Note of the Secretary-General. Available at http://news.dot-nxt.com/docs/Continuation-of-the- Internet-Governance-Forum-final.pdf [accessed 14 April 2012].
5 The Economist (2000) A survey of the new economy: Falling through the Net? For the developing world, IT is more of an opportunity than a threat. Available at http://www. economist.com/node/375645 [accessed 10 April 2012]
6 OECD (2001) Understanding the Digital Divide. p. 5. Available at http://www.oecd.org/ dataoecd/38/57/1888451.pdf [accessed 15 April 2012].
7 G8 (2001) 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. Available at http://www.g7.utoronto.ca/summit/2001genoa/dotforce1.html [accessed 10 April 2012].
8 WEF (2012) Global Information Technology Report. Available at http://www.weforum. org/news/global-information-technology-report-highlights-emergence-new-digital-divide [accessed 17 October 2012].
9 European Union [EU] (no date) Universal Service. Available at http://ec.europa.eu/ information_society/policy/ecomm/current/consumer_rights/universal_service/ index_en.htm [accessed 10 April 2012].
10 According to Internet World Stats (2012) Internet Usage Statistics. The Internet Big Picture. Available at http://www.internetworldstats.com/stats.htm [accessed 20 April 2012].
11 For an overview of the Pacific Islands situation, see Economic and Social Commission for Asia and Pacific [UNESCAP] (2008) Enhancing Pacific Connectivity. United Nations Publications. Available at http://www.unescap.org/idd/Pubs/st_escap_2472.pdf [accessed 20 April 2012].
12 For a study on the impact of IXPs implementation in Kenya and Nigeria, see Internet Society (no date) Internet exchange points (IXPs). Available at http://internetsociety.org/ what-we-do/issues/internet-exchange-points-ixps [accessed 20 April 2012].
13 For a comprehensive survey of interconnection, please consult the study elaborated for the European Commission: Marcus J. and Elixmann D (2008) The Future of IP Interconnection: Technical, Economic and Public Policy

Aspects. WIK-Consult GmbH, Bad Honnef, 29 January 2008. Available at http://ec.europa.eu/information_society/ policy/ecomm/doc/library/ext_studies/future_ip_intercon/ip_intercon_study_final. pdf [accessed 1 February 2012].

14 According to ITU sources, the transfer from developed to developing countries between 1993 and 1998 was US $40 billion. ITU-T Study Group 3 (2000) Accounting Rate Reform undertaken by ITU-T Study Group 3. Available at http://www.itu.int/ITU-T/ studygroups/com03/accounting-rate/ [accessed 20 April 2012].

15 Huston G (2005) Where's the Money? Internet Interconnection and Financial Settlement The ISP Column, January 2005, Internet Society, pp. 7-9. Available at http://www. ictregulationtoolkit.org/en/Document.3302.pdf [accessed 20 April 2012].

16 One of the limitations of negotiating this issue between governments is that most interconnection agreements are concluded between private telecommunication operators. They are often confidential. ITU recommendations are available at http://www.itu.int/ rec/T-REC-D.50/e [accessed 17 October 2012].

17 ITU (2010) Resolution 101. Available at http://www.itu.int/osg/csd/intgov/resoultions_2010/PP-10/RESOLUTION_101.pdf [accessed 17 October 2012].

18 India has announced the launch of a government-subsidised tablet computer of only $35, according to BBC News South Asia (2011) India launches Aakash tablet computer priced at $35. 5 October. Available at http://www.bbc.co.uk/news/world-south-asia-15180831 [accessed 15 April 2012].

19 Ismail S (2006). Analyzing the World Bank's blueprint for promoting information and communications. Federal Communications Law Journal 59(1). Available at http://www.law. indiana.edu/fclj/pubs/v59/no1/13-Book%20ReviewFINAL.pdf [accessed 20 April 2012].

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

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 պե՞տք է վերանայել մարդու իրավունքների ավանդական հայեցակարգերը՝ հաշվի առնելով համացանցի օգտագործումը: Քննարկվում են նաև մարդու «նոր» իրավունքները, ինչպիսին է՝ հեռահաղորդակցության համար իրավունքը:

Համացանցին հասանելիության իրավունքներ

Ֆինլանդիան առաջին երկիրն էր, որն իրավապես երաշխավորեց Համացանցին հասանելության իրավունքը: 2010թ.-ի հուլիսի դրությամբ Ֆինլանդիայի բոլոր քաղաքացիներն մեկ մեգաբիթ լայնաշերտ միացման իրավունք ունեին: Սակայն Համացանցին հասանելիության իրավունքը առավել շատ վիճարկվում է ազատ արտահայտման և տեղեկատվության կապված, քան Համացանցի միացման իրական արագության: Կան տարբեր մանրուքներ Համացանիցն հասանելիությունը մարդու իրավունք դիտարկելու հարցում՝ սկսած հասանելիությունից ենթակառուցվածքին մինչև հասանելիությունը բովանդակությանը, ինչպես ՄԱԿ-ի Մարդու իրավունքների խորհուրդը մատնանշում է իր զեկույցում: Այդուհանդերձ, կան նաև հակադիր կարծիքներ վերջինս մարդու հիմնարար իրավունքների շարքին դասելու, երբ կան մարդիկ, որոնք պայքարում են մաքուր ջրի, բժշկական ուշադրության և սննդի համար: Արդյոք՞ սա միջոցներ և ռեսուրսներ չի տանի՝ հասցեագրելով դրանք մարդու առավել հիմնարար իրավունքների:

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 կարևորությունը4: 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:

Համոզմունքների ազատ արտահայտման և տեղեկատվություն որոնելու, ստանալու ու տարածելու իրավունք

Առցանց ազատ արտահայտման իրավունքը առանձնացվեց 2011/2012 թթ. դիվանագիտական օրակարգում. այն ՄԱԿ-ի Մարդու իրավունքների խորհրդի օրակարգում է: Ազատ արտահայտման իրավունքը նաև քննարկվել է բազմաթիվ միջազգային կոնֆերանսներում:

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 փորձերի5:

Սահմանափակ ֆիզիկական հնարավորություններով մարդկանց իրավունքները33

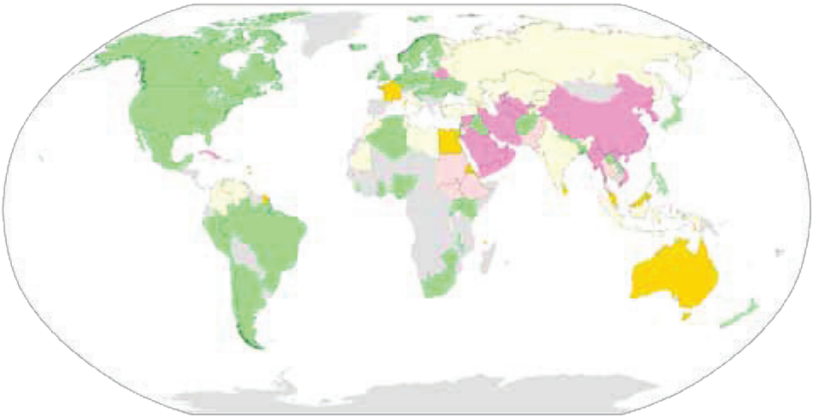
ՄԱԿ-ի գնահատականների համաձայն, աշխարհում սահմանափակ հնարավորություններով 500 մլն մարդ է ապրում: Այս թիվն անընդհատ ավելանում է պատերազմների, կյանքի անբարենաստ պայմանների, հիվանդությունների, դրանց պատճառների, կանխման և բուժման մասին գիտելիքների պակասի պատճառով34: Համացանցը հաշմանդամներին հասարակության 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 153 երկիր ստորագրել է: Այդ պայմանագրում ամրագրված իրավունքները ներկայում ընդգրկվում են ազգային օրենսդրությունների համակարգերում, ինչը մի քանի տարի հետո հնարավորություն կտա ապահովել դրանց կիրառումը35:
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 բաժանմունքը37:
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:

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



Internet censorship by country.

Legend:
- Pervasive censorship
- Substantial censorship
- Selective censorship
- Under surveillance
- No evidence of censorship
- Not classified / No data

Source: **Wikimedia Commons**

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 արգելքը7:
Երրորդ խումբը կազմված է համացանցում քաղաքական գրաքննության օրինակներից: 2012 թ. «Լրագրողներ առանց սահմանի» կազմակերպության ցուցակում թվարկվում էր համացանցում քաղաքական գրաքննություն իրականացնող 14 երկիր8 և 12 երկիր որպես «Համացանցի թշնամի»:

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 է9: 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 մակարդակով10:
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 համակարգերը12: 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 գտնվում13: Տեխնիկական այսպիսի գնահատականը օգնեց դատարանին վերջնական որոշում ընդունել. Yahoo!-ից պահանջեցին զտել Ֆրանսիայից հասանելիությունը դեպի նացիստական նյութեր պարունակող պորտալ:

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 կապը15: 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: Փնտրման զտումը լարվածության առիթ հանդիսացավ Google-ի և Չինաստանի զեկավարության միջև իրականացվում է, ինչի արդյունքում Google-ը 2010թ.-ի հունվարին որոշեց Google.cn-ով կատարված որոնումները վերահղել Հոնգ Կոնգի սերվերների վրա: Այնուամենայնիվ, այդ տարի ավելի ուշ, տեղական օրենքներին ընտելանալու համար Google-ում որոշում են սահմանափակել իրենց տարածաշրջանային վեբկայքերի

որոշ նյութերին հասանելիությունը: Փնտրման արդյունքների զտումն, այնուամենայնիվ, չի բխում միայն կառավարական շրջանակների շահերից, այլև ավել կամ պակաս, ակնհայտորեն կամ թաքնված կերպով կարող է խանգարել նաև առևտրային շահերին: Մեկնաբանները սկսել են քննարկել փնտրողական համակարգերի դերը որպես միջնորդ օգտագործողին տեղեկատվություն տրամադրելու մեջ և զգուշացնել վերջիններիս ազդեցության մասին օգտագործողների գիտելիքների և նախապավությունների վրա:

Վեբ 2.0 մարտահրավեր. 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, You-Tube-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: Հնարավոր լուծումներից մեկը, որ կիրառվել է Մարոկոյում, Պակիստանում, Թուրքիայում և Թունիսում, երկրում You-Tube ներթափանցման լիարժեք շրջափակումն է: Սակայն այդպիսի «մաքսիմալիստական» մոտեցման արդյունքը դառնում է առարկություն չառաջացնող,այդ թվում նաև կրթական նյութերի անհասանելիությունը: Արաբական գարնան իրադարձությունների ընթացքում կառավարությունը դիմեց ծայրահեղ քայլի՝ ամբողջությամբ անջատելով Համացանցին հասանելիությունը սոց կայքերի միջոցով հաղորդակցությունը խանգարելու նպատակով:

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 գիտելիքներ19:
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 պոռնոգրական 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 ներթափանցումը20:

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): Համաձայն որոշ գնահատականների՝ կանխատեսվում է, որ ամբողջ աշխարհում առցանց կրթության շուկան կաճի մոտավորապես 49,6 միլիարդ դոլարով մինչև 2014թ.-ը:
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: Այս առումով կրթական կամակերպությունները սկսեցին զարգացնել ստանդարտներ և ուղեցույցներ առցանց դասախոսութ-յունների դիզայնը և բովանդակությունը գնահատելու համար:

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 (UMAP) 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

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: Դատապարտելի բովանդակությունը հստակորեն նշված է որպես անպատշաճ և անտեղի իրողություն, որոնք ներառում են լայնաբնույթ նյութեր, ներառյալ պոռնոգրաֆիա, ատելություն, բռնություն, ինքնասպանություն քարոզող նյութեր և այլն:

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: 2011թ.-ի տարբեր պլատֆորմաների համար, ներառյալ Microsoft Xbox, Nintendo DS, Nintendo Wii, PC, Playstation, PSP, ամենից լավ վաճառված խաղերից գերակշռել են դաժան խաղերը:

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 ՁԼՄ-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 ՁԼՄ-երի մասնակցությամբ: Ազգային մակարրդակով 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 ԶԼՄ-երի, ակադեմիական միությունների ներկայացուցիչների և «գիտահետազոտական կենտրոնների» որակավորումը: Միջազգային տարբեր կազմակերպություններ, այդ թվում նաև Եվրամիությունը, ՀՄՄ, «Կիբեռաշխարհը» և Diplo-Foundation-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:

Բազմալեզվություն և մշակութային բազմազանություն

Իր գոյության առաջին օրերից համացանցը առավելապես անգլալեզու միջավայր էր: Վիճակագրության համաձայն, համացանցի բովանդակության մոտավորապես 56 տոկոսո անգլերենով նյութերն են, թեև Երկրագնդի բնակչության 70 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 հետ: Որպեսզի համացանցից օգտվել կարողանան ոչ միայն էլիտան, այլև բնակչության ավելի լայն շերտերը, նյութերը պետք է մատչելի ու հասանելի լինեն տարբեր լեզուներով:

Հարցեր

Ոչ-լատինատառ այբուբեն

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:

Մեքենայական թարգմանություններ

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:

Համապատասխան կանոնավորող շրջանակներ

Բազմալեզվության զարգացումը պահանջում է համապատասխան կանոնավորող շրջանակների ստեղծում: Այդ ոլորտում կարևոր դեր է կատարում ՅՈՒՆԵՍԿՕ, 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 առանց 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:

Ծանոթագրություններ

The APC Internet Rights Charter includes Internet access for all; freedom of expression and association; access to knowledge; shared learning and creation – free and open source software and technology development; privacy, surveillance and encryption; governance of the Internet; awareness, protection and realisation of rights. Available at http://www.apc. org/en/node/5677 [accessed 20 March 2012].

2 CNN Tech (2010) First nation makes broadband access a legal right. Available at http:// articles.cnn.com/2010-07-01/tech/finland.broadband_1_broadband-access-internet-access-universal-service?_s=PM:TECH [accessed 20 March 2012].

3 UN General Assembly (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_ en.pdf [accessed 30 April 2012].

4 For a discussion of the UN report see Wagner A (2012) Is Internet access a human right? The Guardian. Available at http://www.guardian.co.uk/law/2012/jan/11/is-internet-access-a-human-right [accessed 20 March 2012].

5 Council of Europe (2010) Convention for the Protection of Human Rights and Fundamental Freedoms. Available at http://conventions.coe.int/treaty/en/treaties/ html/005.htm [accessed 30 April 2012].

6 The Council of Europe adopted the following main declarations of relevance for human rights and the Internet:

• The Declaration on Freedom of Communication on the Internet (28 May 2003). Available at https://wcd.coe.int/ViewDoc.jsp?id=37031 [accessed 20 March 2012].

• The Declaration of Human Rights and the Rule of Law in the Information Society (13 May 2005). Available at https://wcd.coe.int/ViewDoc.jsp?id=849061 [accessed 20 March 2012].

• The Declaration on the Digital Agenda for Europe (29 September 2010). Available at https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2829.09.2010_1%29&Language=lanEnglish&Ver=original [accessed 20 March 2012].

7 Council of Europe (2001) Convention on Cybercrime. Available at http://conventions. coe.int/Treaty/en/Treaties/html/185.htm [accessed 30 April 2012].
8 The Universal Declaration of Human Rights. Available at http://www.un.org/en/ documents/udhr/ [accessed 30 April 2012].
9 Freedom House (2009) Freedom on the Net. A Global Assessment of Internet and Digital Media. Available at http://www.freedomhouse.org/sites/default/files/Freedom%20 OnThe%20 Net_Full%20Report.pdf [accessed 20 March 2012].
10 Valuable comments and inputs were provided by Jorge Plano.
11 UN Enable (no date) World Programme of Action Concerning Disabled Persons. Available at http://www.un.org/disabilities/default.asp?id=23#current [accessed 3 April 2012].
12 Convention on the Rights of Persons with Disabilities. Available at http://www.un.org/ disabilities/default.asp?navid=14&pid=150 [accessed 30 April 2012].
13 IGF, Dynamic coalition on accessibility and disability. Available at http://www. intgovforum.org/cms/index.php/dynamic-coalitions/80-accessibility-and-disability [accessed 30 April 2012].
14 ISOC Disability and Special Needs Chapter. Available at http://www.isocdisab.org/ [accessed 30 April 2012].
15 ICDRI. Available at http://www.icdri.org/ [accessed 30 April 2012].
16 WAI. Available at http://www.w3.org/WAI/ [accessed 30 April 2012].
17 ISOC, Universal Design for the Internet. Available at http://www.isoc.org/briefings/002/ [accessed 30 April 2012].
18 Zick T (1999). Congress, the Internet, and the intractable pornography problem: the Child Online Protection Act of 1998, Creighton Law Review, 32, pp. 1147, 1153, 1201. Available at http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1873&context=facpubs [accessed 2 April 2012].
19 For a discussion of Internet gambling, see: Girdwood S (2002) Place your bets ... on the keyboard: Are Internet casinos legal? Campbell Law Review 25. Available at http://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1398&context=clr [accessed 2 April 2012].
20 For a full listing and related articles see the Reporters

without Borders Internet dedicated page available at http://en.rsf.org/internet.html [accessed 2 April 2012]. The complete 2012 report is available at http://en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html [accessed 2 April 2012].

21 As compiled by Wikimedia Commons (2012) to reflect the latest information reported by Reporters without Borders and OpenNet Initiative. Available at http://en.wikipedia.org/ wiki/File:Internet_Censorship_World_Map.svg [accessed 2 April 2012].

22 The OpenNet Initiative has documented network filtering of the Internet by national governments in over forty countries worldwide. See Noman H and York J (2011) West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011 OpenNet Initiative Bulletin. Available at http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011 [accessed 2 April 2012].

23 For more information about Platform for Internet Content Selection (PICS), see Resnick P and Miller J (1996) PICS: Internet Access Controls Without Censorship. Available at http:// www.w3.org/PICS/iacwcv2.htm [accessed 2 April 2012].

24 For an overview of available filtering types, see the National Academy of Sciences dedicated page available at http://www.nap.edu/netsafekids/pro_fm_filter.html [accessed 2 April 2012].

25 Although Vint Cerf participated in the panel, he objected to the final report, which he said 'did not focus on the flaws or the larger implications of installing online gates'. Source: Guernsey L (2001) Welcome to the world wide web, passport, please? New York Times, 15 March 2001. Available at http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html?pagewanted=all&src=pm [accessed 2 April 2012].

26 Akami claims that it can identify people's geographical location as far as their ZIP codes. This is the technological limit. Information about street addresses cannot be obtained from IP numbers. 'Silicon Valley's Quova Inc., one of the leading providers of this technology, claims it can correctly identify a computer user's home country 98 percent of the time and the city about 85 percent of the time, but only if it's a large city. Independent studies have pegged the accuracy rate of such programs, which also are sold by companies such as InfoSplit, Digital Envoy, Netgeo, and Akami, at

70 to 90 percent'. Source: Cha AE (2002) Rise of Internet borders prompts fears of web's future. Washington Post, 4 January, p. E01.
27 Knight W (2002) Google keywords knock Chinese surfers offline. New Scientist Internet edition, 13 September. Available at http://www.newscientist.com/article/dn2797-google-keywords-knock-chinese-surfers-offline.html [accessed 2 April 2012].
28 Knight W (2002) On-off access for Google in China. New Scientist Internet edition, 13 September. Available at http://www.newscientist.com/article/dn2795-onoff-access-for-google-in-china.html [accessed 2 April 2012].
29 Drummond D (2010) An update on China, 28 June 2010. The Official Google Blog. Available at http://googleblog.blogspot.com/2010/06/update-on-china.html [accessed 2 April 2012].
30 A good starting point to this debate is Mary Murphy's blog post on DiploFoundation's Internet Governance blog channel and the comments raised upon: Google...stop thinking for me! Available at http://www.diplomacy.edu/blog/googlestop-thinking-me [accessed 10 April 2012].
31 Jiang Y (2011) Consumer Video Understanding: A Benchmark Database and An Evaluation of Human and Machine Performance ICMR'11. April 17-20, Trento, Italy. Available at http:// www.ee.columbia.edu/~yjiang/publication/icmr11-consumervideo.pdf [accessed 2 April 2012].
32 Crete-Nishihata M and York J (2011) Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking. OpenNet Initiative. Available at http://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking [accessed 2 April 2012].
33 Council of Europe (2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Available at http://conventions.coe.int/Treaty/en/Treaties/html/189. htm [accessed 30 April 2012].
34 EU Information Society (no date) Safer Internet action plan. Available at http:// ec.europa.eu/information_society/activities/sip/index_en.htm [accessed 14 November 2008].
35 Lessig L (1996) The Zones of Cyberspace. Stanford Law Review 48 pp. 1403, 1405.

36 Steve A (no date) Church of Scientology censors net access for members Available at http:// www.xenu.net/archive/events/censorship [accessed 2 April 2012].
37 Nagel D (2010), The Future of E-Learning Is More Growth. Campus Technology. Available at http://campustechnology.com/articles/2010/03/03/the-future-of-e-learning-is-more-growth.aspx [accessed 3 April 2012].
38 GATS. Available at http://www.wto.org/english/res_e/booksp_e/analytic_index_e/ gats_01_e.htm#article1A [accessed 30 April 2012].
39 For a comprehensive study of the interpretation of GATS related to higher education see Tilak J (2011) Trade in higher education: The role of the General Agreement on Trade in Services (GATS). UNESCO: International Institute for Educational Planning. Paris. Available at http://unesdoc.unesco.org/images/0021/002149/214997e.pdf [accessed 3 April 2012].
40 For a sample list of organizations and works dealing with recommendations and standards for e-learning see Bates T (2010) E-learning quality assurance standards, organizations and research. Available at http://www.tonybates.ca/2010/08/15/e-learning-quality-assurance-standards-organizations-and-research/ [accessed 3 April 2012].
41 European Commission (no date). ECTS. Available at http://ec.europa.eu/education/ lifelong-learning-policy/ects_en.htm [accessed 3 April 2012].
42 UMAP (no date). UMAP. Available at http://www.umap.org/en/cms/detail.php?id=106 [accessed 3 April 2012].
43 This text was prepared by Vladimir Radunovic for the Advanced Course on Cybersecurity and Internet Safety (Internet Governance Capacity Building Programme – DiploFoundation).
44 Reilly J (2012) The Best-Selling U.S. Games Of 2011. gameinformer. Available at http:// www.gameinformer.com/b/news/archive/2012/01/12/these-are-the-10-best-selling-u-s-games-in-2011.aspx [accessed 12 April 2012].
45 Insafe. Available at http://www.saferinternet.org/web/guest/home [accessed 30 April 2012].
46 CyberSmart. Available at http://www.cybersmart.org/ [accessed 30 April 2012].

47 IKeepSafe. Available at http://www.ikeepsafe.org/ [accessed 30 April 2012].
48 I-Safe. Available at http://www.isafe.org/ [accessed 30 April 2012].
49 NetSmartz. Available at http://www.netsmartz.org/Parents [accessed 30 April 2012].
50 EU2009. Prague Declaration for a Safer Internet for Children. Available at http:// ec.europa.eu/information_society/activities/sip/docs/events/prague_decl.pdf [accessed 30 April 2012].
51 ITU (no date) Global Cybersecurity Agenda. Available at http://www.itu.int/osg/csd/ cybersecurity/gca/ [accessed 30 April 2012].
52 According to W3Techs (2012) Usage of content languages for websites. Available at http:// w3techs.com/technologies/overview/content_language/all [accessed 3 April 2012].
53 For more information regarding multilingualism on the Internet please consult the following study: AlShatti Q, Aquirre R and Cretu V (2007) Multilingualism - the communication bridge. DiploFoundation's Internet Governance Research Project, 2006/2007. Available at http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus. diplomacy.edu/thina/txgetxdoc.asp?IDconv=3241 [accessed 3 April 2012].
54 Unicode Consortium. Available at http://unicode.org/ [accessed 30 April 2012].
55 UNESCO (2001) Universal Declaration on Cultural Diversity. Available at http:// portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_ SECTION=201.html [accessed 30 April 2012].
56 Creative Commons is a non-profit organisation that develops, supports, and stewards legal and technical infrastructure that maximizes digital creativity, sharing, and innovation. Available at http://creativecommons.org/ [accessed 3 April 2012].
57 For more information regarding the Internet as a global public good, please consult the following study: Seiiti A and Psaila S (2006) The Protection of the Public Interest with regards to the Internet. DiploFoundation's Internet Governance Research Project, 2005/2006. Available at: http://archive1.diplomacy.edu/poolbin.asp?IDPool=128 [accessed 3 April 2012].

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 էին1: 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 կառուցվել է IETF-ի, ISOC-ի և ICANN-ի ներքո: 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 չէ2: 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

Համացանցի կառավարում. մեկ փոփոխականի երկրաչափություն

Համացանցի կառավարումը պահանջում է տարբեր շահառուների ներգրավվածություն շատ բնագավառներում, այդ թվում, միջազգային իրավական հզորություն, Համացանցի կառավարման տվյալ հարցում հետաքրքրվածություն և հասանելի փորձառություն: Նման բազմազանությունը կարող է տեղավորվել մեկ Համացանցի կառավարման համակարգում՝ օգտագործելով փոփոխական երկրաչափության մոտեցումները: Այս մոտեցումը, որն արտացոլում է շահառուների հետաքրքրությունները, նախապատվությունը և Համացանցի կառավարման հարցերը լուծելու կարողությունները, իրականացված է WSIS-ի 49 հոդվածում, որը բնութագրում է հիմնական շահառուների հետևյալ դերերը.

- վիճակներ- քաղաքականության մարմին Համացանցի հանրային քաղաքականության հարցերի համար,
- մասնավոր ոլորտ- Համացանցի զարգացում տեխնիկական և տնտեսական բնագավառներում,
- քաղաքացիական հասարակություն- համայքային մակարդակում Համացանցի դերի կարևորությունը,
- միջկառավարական կազմակերպություն- Համացանցին վերաբերող հանրային քաղաքականության հարցերի կոորդինացում,
- միջազգային կազմակերպություն - Համացանցի տեխնիկական ստանդարտների և համապատասխան քաղաքականությունների մշակում:

փոխզիջման արդյունքը WGIG-ի հաջողությունն էր: WSIS-ի ավարտից հետո համացանցի կառավարումը մնում 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 կառուցվածքը նման է WGIG-ին. այդ կառուցվածքները միջազգային մակարդակում բազմակողմ գործընկերութան օրինակներ են մնում:
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 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 բանավեճերին4:

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

Մալուխի աշխարհաքաղաքական ռազմավարությունը և քաղաքականությունը

Անգլոֆրանսիական Անտանտը հիմնվել է 1904 թվականին: Գերմանիայի հետ սերտ համագործակցություն հաստատելով՝ այնուամենայնիվ, Ֆրանսիայի հեռագրային նախարարությունը չհետևեց երկրի արտաքին քաղաքականությանը: Գլխավոր պատճառը Բրիտանիայի գերիշխանությունը գլոբալ «մալուխային աշխարհաքաղաքական ռազմավարության» մեջ կրճատելն էր՝ Գերմանիայի հետ նոր հեռագրային մալուխներ պատրաստելով: Ֆրանսիացի պատմաբան Չարլզ Լեսաժը այս քաղաքականության վերաբերյալ արեց հետևյալ մեկնաբանությունը.«Հեռագրային քաղաքականության և Ֆրանսիական դիվանագիտության միջև երկարատև տարաձայնությունները, կարծում եմ, գալիս են այն փաստից, որ այս երկրում յուրաքանչյուր նախարարություն ունի իր արտաքին քաղաքականությունը. Արտաքին գործերի նախարարությունն իրենը, Ֆինանսներինը՝ իրենը... Փոստային և հեռագրային նախարարությունը անցյալ մի քանի տարվա ընթացքում ունի իր արտաքին քաղաքականությունը՝ առանց Անգլիային թշնամանալու, այլ ցույց տալով իր ուժեղ ուղղվածությունը դեպի Գերմանիա»:

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:

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, արևւտրի 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 CORE1 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 նոտայով7: 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. սեպտեմբերին, 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, IANA2-ի վերաբերյալ համաձայնագիրն այժմ վերանայման փուլում է.:

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

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 հարցերով10: 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:

Առևտրի միջազգային պալատ (ICC)

Առևտրի միջազգային պալատը (ICC), առավել հայտնի որպես տարբեր բնագավառների և աշխարհագրական սահմանների բիզնեսի ներկայացման հիմնական կազմակերպություն, իրենից ներկայացնում է գլոբալ Համացանցի կառավարման գործընթացներում բիզնեսի հիմնական ներկայացուցիչ: ICC ակտիվորեն ներգրավված է եղել WGIG-ի և WISIS-ի վաղ բանակցություններում, և շարունակում է մնալ IGF-ի ներկա գործընթացի ակտիվ մասնակից:

Դոմենային անուններով զբաղվող 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:

Համացանցային ծառայությունների մատակարարներ (ISPs)
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 ընկերակցությունը (ITAA) և այլն:

Հեռահաղորդակցային ընկերություններ

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:

Ծրագրային ապահովման ընկերությունները

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:

Համացանցի բովանդակության ընկերություններ

Ընդգրկում է համացանցի հիմնական ապրանքանիշերը, ինչպիսիք են՝ Google-ը,Facebook-ը և Twitter-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:

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: 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: Քաղաքացիական հասարակությունը շարունակեց ակտիվորեն ներգրավվել IGF-ի գործունեության մեջ: Համացանցի կառավարման գործընթացում քաղաքացիական հասարակության ներկայացման յուրահատուկ ձևերից է Համացանցի կառավարման աջակցությունն է (IGC), որը ենթադրում է հետաքրքր-ված անհատների կարծիքների փոխանակում, Համացանցի կառավարման ցուցակում քննարկվող հար-ցերի քաղաքականության տարբերակների և փորձաքննության մշակում:

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 բնագավառում 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):

ՀԿ-ները և WSIS-ը

ՀԿ-ների մասնակցությունը WSIS-ում հարաբերականորեն ցածր է: 3000 ՀԿ-ներից, որոնք ՄԱԿ-ի ՏՍԽ-ում ունեին խորհրդատվական կարգավիճակ, WSIS-ին մասնակցում էին միայն 300-ը:

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:

Տեխնիկական 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 հիմնված 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 միությունները իրենցից ներկայացնում են էպիսթեմիկ միություն11: 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), 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): 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 2000-2007թթ.: 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

Տերմինաբանություն

Այլ տերմիններն օգտագործվում են տեխնիկական միավորումների հետ փոխադարձ փոխարինելիության սկզբունքով, ինչպիսիք են Համացանցի միավորում, Համացանցի մշակողներ, Համացանցի հիմնադիրներ, Համացանցի հայրեր, և տեխնոլոգներ: Տեխնիկական միավորում տերմինն օգտագործվում է WSIS-ի հայտարարագրերում և այլ քաղաքականության փաստաթղթերում:

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 հիմն ական կառույցն է: Դրա պատասխանատվության ոլորտում ընդգրկվում է դոմենային անունների համակարգի կառավարումը (DNS)՝ համացանցի հիմն ական ենթակառուցվածքը, որը կազմված է IP հասցեներից, դոմե նային անուններից և արմատական սպասարկուներից: ICANN-ի հանդեպ հետաքրքրությունն աճել է 2000-ականներին համացանցի արագ աճի հետ մի ասին, 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 կողմե րը, այդ պատճառով ճիշտ չէ այն անվանել «համացանցի կառավարություն», ինչը հաճախ են անում: ICANN-ը կառավարում է համացանցային ենթակառուց-վածքը, 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 մի ավորում է: Դրա գործառնական լիազորություն-ները հիմն ված են ԱՄՆ առևտրի նախարարության և ICANN-ի մի ջև փոխըմբռնման

մասին հուշագրի
վրա, որը ստորագրվել է 1998 թ. և երկու անգամ երկարացվել (երկրորդ անգամ՝ 2006 թ. սեպտեմբերից մի նչև 2009 թ. սեպտեմբերը): 2009 թ.հոկտեմբերի 1-ի դրությամբ ICANN-ի գործառնության պաշտոնա-կան 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 հիմն ական խմբի: Առաջին խումբը կազմված է
նրանցից, ովքեր ICANN-ի գործունեությանը մասնակցել են ստեղծման պահից՝ համացանցային մի ությունները, գործարար մի ությունները և ԱՄՆ կառավարությունը: Երկրորդ խումբն ընդգրկում է մի ջկառավարական կազմակերպություններ, որոնց շարքում կարևոր դեր են կատարում Հեռահաղորդակ-ցության մի ջազգային մի ությունը և Մտավոր սեփականության համաշխարհային կազմակերպությունը:
Երրորդ խումբը կազմված է ազգային կառավարություններից, որոնք 2003թ. WSIS-ից սկսած ցանկա-նում են առավել նշանակալի դեր խաղալ ICANN-ում:
Չորրորդ խումբը ներառում է համացանցի օգտատերերին («բոլորի մի ություն»): 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 իրավա-կան 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 օգտատե-րերին՝ կառավարման «բոլորին ներկայացնող» (atlarge) կառույցի մի ջոցով: Կազմակերպչական այդ փորձը դեռևս շարունակվում է:

ICANN-ում որոշումներ ընդունելու գործընթացի վրա ազդեցություն են գործել համացանցի կառավար-ման վաղ շրջանի մոդելները, որ հիմնված էին ժողովրդավարության, թափանցիկության, բաց լինելու և համընդհանուրի մասնակցության սկզբունքների վրա: ICANN-ում որոշումն եր ընդունելու հարցում 1980-ականների համացանցային մի ությունների և ներկա համատեքստի մի ջև հիմն ական տարբերությունը «սոցիալական կապիտալի» մակարդակն է: Նախկինում համացանցային մի ությունը փոխադարձ վստահության և համե րաշխության ավելի էր արժանանում, ինչը նշանակալիորեն հեշտացնում էր որոշումներ ընդունելու և վեճերը լուծելու գործընթացը: Համացանցի տարածումը հանգեցրեց շահագր-գիռ կողմերիբազմազանության և քանակի ավելացման, համապատասխանաբար, այդ մասնակիցների սոցիալական կապիտալի մակարդակը շատ ցածր է: Այդ պատճառով համացանցի զարգացման սկզբնական փուլերում գոյություն ունեցող որոշումն եր ընդունելու ընթացակարգը պահպանելու մասին
համացանցային միության պահանջը, հիմնականում, ուտոպիական է: Առանց սոցիալական կապիտալից կախվածության, որոշումն եր ընդունելու գործընթացի գործառնությունն ապահովելու միակ միջոցը զսպելու և հակակշռելու տարբեր մե խանիզմն երի 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 կոմի տեի ուժեղացումը և անմիջական քվեարկության համակար-գից 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-ով12: 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 For a comprehensive overview of the diverse attempts of classifications and mapping of Internet Governance issues and actors see Souter D (2010) Mapping internet public policy APC Symposium on Networking Networks in Internet Public Policy, Ancona, July 2010. Available at http://www.apc.org/en/system/files/APCMappingInternetPublicPolicy_ Slides.pdf [accessed 27 April 2012].

2 The exception was the government of the United States and a few developed countries (Australia, New Zealand and, at that time, the European Commission).

3 The WSIS process started with the first preparatory meeting held in July 2002 in Geneva. The first summit was held in Geneva (December, 2003) and the second summit in Tunisia (November, 2005).

4 The selection of the members of WGIG combined both representation and expertise criteria. The representation structure was guided by a principle of one-third of participants from governments, civil society, and the business sector. Government representatives were selected according to the usual criteria of the UN regional groups. While observing the representation aspect, the selected members were supposed to be knowledgeable about the subject in order to contribute substantially to the WGIG discussion.

5 The Brazilian model of the management of its country domain name is usually taken as a successful example of a multistakeholder approach. The national body in charge of Brazilian domains is open to all users, including government authorities, the business sector, and civil society. Brazil gradually extended this model to other areas of Internet governance, especially in the process of the preparation for the IGF-2007, which was hosted in Rio de Janeiro.

6 Lesage C (1915), La rivalite franco-britannique. Les cables sous-marins allemands Paris. p. 257-258; quoted in: Headrick D (1991), The Invisible Weapon: Telecommunications and International Politics 1851-1945 Oxford: Oxford University Press. p. 110.

7 US Secretary of State criticizing ITU for the initiative: 'without authorization of member governments to hold a global meeting involving an unauthorized expenditure of resources and concluding 'international agreements.' Quoted in Drake W. (2004) Reframing Internet Governance Discourse: Fifteen Baseline Propositions, p. 9. Available at http://www.un-ngls.org/orf/drake.pdf [accessed 24 April 2012].

8 The convenience of 'one-stop shopping' was one of the arguments for establishing the ITU as the central Internet governance player.

9 Valuable comments were provided by Ayesha Hassan.

10 The technical community fulfils all the criteria in Peter Haas's definition of an epistemic community: a professional group that believes in the same cause and effect relationships, truth test to accept them, and shares

common values; its members share a common understanding of the problem and its solutions. Haas P (1990) Saving the Mediterranean: the politics of international environmental co-operation. New York: Columbia University Press, p. 55.12 Network Solutions is a technology company founded in 1979. The domain name registration business has become the most important division of the company, but currently it has diversified its portfolio to include web services for small businesses. For more information see Network Solutions presentation website. Available at http://about. networksolutions. com/ [accessed 24 April 2012].

12 Esther Dyson's response to Ralph Nader's Questions (15 June 1999). Available at http:// www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm [accessed 24 April 2012].

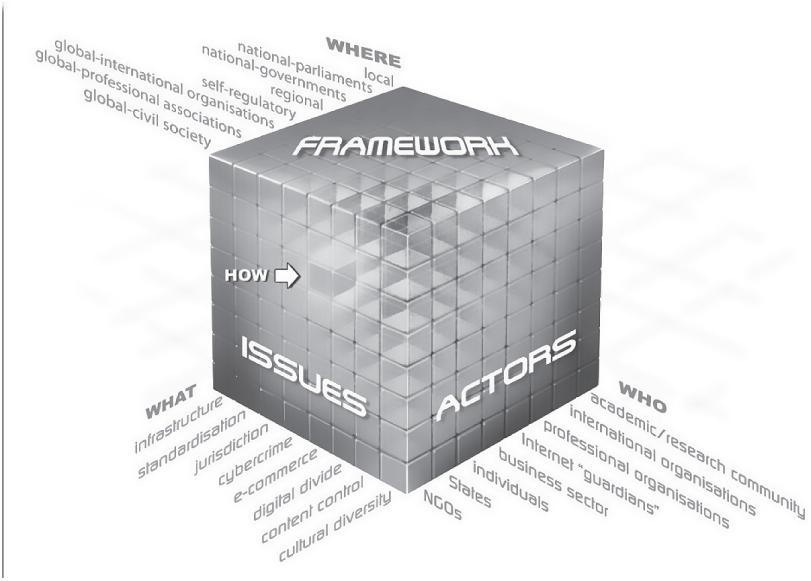
Բաժին 8

Հավելված

Հավելված

Ճանապարհորդություն դեպի Համացանցի կառավարում

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):

Ծրագրային ապահովում- 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

5-րդ հրատարակություն

Ձևավորումը՝ Զորան Մարչետիչ, Կարեն Կարապետյան
Հրատ. ղեկավար՝ Իգոր Մկրտումյան
Հրատ. խմբագիր՝ Հայկազ Բաղյան
Գիտ. խմբագիր՝ Նարինե Խաչատրյան
Թարգմանիչ՝ Անի Բաղյան

«Նոյյան Տապան» տպագրատուն
Թուղթ՝ օֆսեթ N1, 60x84 1/16 ծավալը՝ 4,875 տպ. մամուլ
ստորագրված է տպագրության 13/02/12, տպաքանակը՝ 1000
ՀՀ, Երևան 0009, Իսահակյան 28, հեռ.՝ (+37410) 565965
E-mail: contact@nt.am
URL: http://www.nt.am