Azərbaycan Milli Elmlər Akademiyası

İNFORMASİYA TEXNOLOGİYALARI
İNSTİTUTU

Rasim Əliquliyev
Rasim Mahmudov

İNTERNETİN TƏNZİMLƏNMƏSİ PROBLEMLƏRİ

EKSPRESS-İNFORMASİYA

İNFORMASİYA CƏMİYYƏTİ
SERİYASI

Bakı – 2010

Əliquliyev R.M., Mahmudov R.Ş. İnternetin tənzimlənməsi problemləri. Ekspress-informasiya. İnformasiya cəmiyyəti seriyası.
Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2010, 115 səh.

Tədqiqat işində İnternetin tənzimlənməsi zərurəti və problemləri araşdırılır. Müvafiq tənzimləmə sahəsində beynəlxalq təşəbbüslər, qabaqcıl ölkələrin təcrübəsi analiz edilir. Tənzimləmə zamanı tətbiq edilən üsullar, hüquqi mexanizmlər və yurisdiksya məsələləri öyrənilir. Həmçinin İnternetlə bağlı digər problemlər - şəxsi həyatın toxunulmazlığı və fərdi məlumatların qorunması, domen adları sisteminin idarə edilməsi, provayderlərin hüquqi məsuliyyətinin müəyyənləşdirilməsi, kibercinayətkarıqla, spamlarla mübarizə, intellektual mülkiyyət hüquqlarının qorunması, elektron kommersiya fəaliyyətinin tənzimlənməsi məsələləri tədqiq edilir.

AMEA İnformasiya Texnologiyaları İnstitutunun Elmi Şurasının qərarı ilə çapa tövsiyə olunmuşdur.

Elmi redaktor: t.e.n. Rəşid Ələkbərov

ISBN: 978-9952-434-23-1

MÜNDƏRİCAT

GİRİŞ

Hazırda bəşəriyyətin qarşısında dayanan ən mühüm vəzifələrdən biri qlobal informasiya cəmiyyətinin qurulmasıdır. İnformasiya cəmiyyətinin qurulmasında isə İnternet həlledici rol oynayır. Başqa sözlə desək, İnternet informasiya cəmiyyətinin əsas dayağı kimi qloballaşan dünyada ən mühüm fenomenə çevrilməkdədir. Bu rəqəmsal texnologiya nəhəng informasiya, bilik potensialını özündə əks etdirir, bəşəriyyətin milli-mədəni sərhədləri aşaraq, vahid qlobal cəmiyyətdə birləşməsinə gətirib çıxarır. Qlobal İnternet şəbəkəsinin yaratdığı geniş imkanlar insanların düşüncə tərzində, iş üsulunda, ünsiyyətində və sosial fəaliyyətində böyük dəyişikliklərə səbəb olur.

Bütün bunların nəticəsində İnternet coğrafi sərhədlərə əsaslanan beynəlxalq hüquq normalarını və milli qanunları gücsüz vəziyyətə gətirir. İnternet texnologiyalarının imkanları hesabma formalaşan virtual münasibətləri real dünya qanunları ilə idarə etmək xeyli çətinləşir və bəzi hallarda hətta mümkün olmur. Virtual münasibətlərin tənzimlənməsi bu mühitə xas olan yeni qanunların, normaların yaradılmasını, tətbiq edilməsini zəruri edir.

İnternetin ayrı-ayrı seqmentlərinə mnünasibətdə dövlət yurisdiksiyasının hüdudları ilə bağlı problem müasir hüququn ən mürəkkəb və mühüm məsələlərindən biridir. Burada iki yanaşma mövcuddur. Birincisi həm ölkə daxilində, həm də ölkə hüdudlarından kənarda İnternet vasitəsilə ötürülən informasiya üzərində sərt nəzarətin (senzuranm) tətbiqini nəzərdə tutur. Digər yanaşma İnternetə informasiya mübadiləsi və istifadəçilərə maksimal əlverişli şərait rejimi yaratma vasitəsi kimi

hüquqi tənzimləmə çərçivəsi müəyyən etməklə hərtərəfli dövlət tənzimlənməsindən ibarətdir. Bu sistemdə həmin çərçivənin maksimum genişləndirilməsinə çalışan bir çox hüquq-müdafiə təşkilatları fəaliyyət göstərir.

Bəzi ölkələr hesab edirlər ki, əgər informasiya resursu onların vətəndaşları üçün əlyetərlidirsə, deməli, serverin fiziki yerləşdiyi yerdən asılı olmayaraq, onların yurisdiksiyasına aiddir. Məsələn, Fransa və Avstraliya məhkəmələrinin qərarlarına görə, ABŞ saytları həmin ölkələrin yurisdiksiyasında yerləşir, ona görə də bu ölkələrin qanunlarına tabe olmalıdır [1]. Nəticədə bütün dünyada provayderlər çətin vəziyyətə düşürlər. Onlar fiziki olaraq yerləşdiyi dövlətlərlə yanaşı, bir sıra digər dövlətlərin yurisdiksiyasına da əməl etməli olurlar.

Transmilli fəaliyyət milli qanunvericiliklərlə beynəlxalq praktika arasında ziddiyyət yaradır. Hər bir ölkə öz yurisdiksiyası çərçivəsində qanunlar qəbul etmək və onları tətbiq etmək hüququna malikdir. Yəni bu, onların suveren hüquqlarıdır, yaxud dövlət suverenliyinin əsas prinsiplərindən biridir. Lakin elə şərait yaranır ki, bu suveren hüquq şübhə altına düşür və ziddiyyət meydana çıxır. Bəzi hallarda müvafiq ziddiyyət xaricdən olan böyük fəallıq hesabına yaranır. Yəni fəaliyyət müvafiq yurisdiksiya hüdudlarından kənarda həyata keçirilirsə, həmin yurisdiksiyanın qanunları tətbiq etmə qabiliyyətinə təsir göstərir.

Bundan başqa, İnternet istifadəçilərinin bir hissəsi qlobal şəbəkədə "məkansızlıq" ("ləməkan") ideyasını yayaraq, özlərinin qanundan və dövlətdən asılı olmadıqlarını bəyan edirlər və "suveren şəbəkə" uğrunda mübarizə aparırlar. Yəni İnternet cəmiyyətlərinin nümayəndələri arasında belə bir fikir də geniş yayılıb ki,

bu qlobal şəbəkənin tənzimlənməsi vacib deyil, hətta qeyri-mümkündür. Həmin baxışlara görə, İnternet şəxsiyyətlərarası unikal ünsiyyət vasitəsidir və heç bir dövlətə mənsub deyil. İnternet resurslarına çıxış xüsusi hüquqlara aid olduğuna görə, onun qarşısında hər-hansı inzibati maneə qoyula bilməz. Onların fikrincə, İnternet – tamamilə özünütənzimləyən informasiya mühitidir. Onun istifadəçiləri bu qlobal resursdan istifadə qaydalarını sərbəst şəkildə müəyyən etməlidirlər.

İnternetin inkişafının ilk vaxtlarında hətta belə bir fikir yayılmışdı ki, bu qlobal şəbəkə milli sərhədləri aşacaq və dövlət suverenliyi prinsipini pozacaq. Qlobal şəbəkədə söz azadlığının müdafiəsi, kiberməkanda sosial və hüquqi problemlərin tədqiqi ilə məşğul olan Elektron Sərhəd Fondunun (*Electronic Frontier Foundation*) yaradıcısı və vitse-prezidenti Con Perri Barlou özünün məşhur "Kiberməkanın müstəqilliyi" adlı Bəyannaməsində bütün dövlətlərə belə bir müraciət ünvanlamışdı: "Bizim aramızda sizə yer yoxdur. Bizim toplandığımız yerdə siz yuxarı hakimiyyətə malik deyilsiniz. Bizim üzərimizdə hökmranlıq etməyə sizin nə mənəvi haqqınız, nə də məcburetmə metodunuz var. Siz nə bizi, nə də bizim dünyamızı tanımırsınız. Kiberməkan sizin sərhədlərinizdən kənarda yerləşir" [1].

Lakin dövlətlər bu cür bəyanatlara fikir vermədilər və öz yurisdiksiyalarında söz azadlığma senzura tətbiq etmək üçün qanunlar qəbul etdilər. Bu zaman xəbərdarlıq edildi ki, bir yurisdiksiyada tətbiq edilən qaydalar digər yurisdiksiyalar üçün zərərli effekt verə bilər. Bu isə həm İnternetin fəaliyyətinə mənfi təsir göstərə, həm də vətəndaş hüquqlarının pozulmasına səbəb ola bilər. Bu tövsiyələr də rədd edildi. Nəhayət, etiraf edildi ki, İnternet heç də unikal

bir sfera deyil, transmilli fəaliyyət həmişə tənzimləməyə cəlb edilib.

Bu etirafdan sonra yeni təşəbbüslər yarandı. İnterneti kütləvi yayım vasitəsi kimi tənzimləmək və artıq televiziyaya nəzarət sahəsində mövcud olan metodları (siyasi senzura, filtirasiya) tətbiq etmək cəhdləri meydana gəldi. Həmçinin dövlətlər İnterneti telefon sistemi kimi tənzimləməyə cəhd edirlər. Bundan başqa, dövlət hakimiyyət orqanları müəllif hüquqları rejimini, diffamasiya və böhtan haqqında qanunları "aktuallaşdıraraq", onları yeni kommunikasiya infrastrukturunda tətbiq etməyə başlayırlar.

Müxtəlif səbəblərdən İnternetin fəaliyyətini tənzimləyən ölkələrin sayı durmadan artır. Buna səbəb kimi "milli təhlükəsizliyin təmin edilməsi", "milli-mədəni normaların və dini dəyərlərin mühafizə edilməsi", "uşaqların pornoqrafiyadan və istismardan qorunması", "intellektual mülkiyyət hüquqlarınm müdafiəsi" kimi arqumentlər irəli sürülür.

İnternetin unikallığı ondan ibarətdir ki, hər hansı hüquqi və ya fiziki şəxsin, yaxud dövlətin mülkiyyətində deyil. Ona görə də bu qlobal şəbəkənin heç bir seqmentində mərkəzləşdirilmiş tənzimləmə, senzura və digər informasiyaya nəzarət metodları mövcud deyil. Bunun hesabına istənilən informasiyanı heç bir məhdudiyyət olmadan əldə etmək imkanı yaranır ki, nəticədə də informasiya sahiblərinin hüquqlarının pozulması halları əhəmiyyətli dərəcədə artır. Ona görə də informasiya təhlükəsizliyinin təmin edilməsi problemi və kompyuter cinayətkarlığı ilə mübarizə sisteminin yaradılması hazırda xüsusi aktuallıq kəsb edir.

İnternet söz azadlığının reallaşdırılması üçün də əvvəllər mümkün olmayan imkanlar yaradır. Lakin yeni azadlıq formasının meydana gəlməsi şəraitində şəxsi həyatın toxunulmazlığı, şəxsi məlumatların təhlükəsizliyi və söz azadlığı getdikcə daha çox pozulmaqdadır. Bu gün İnternetdən hüquqazidd istifadəyə dair faktları heç kim təkzib edə bilməz. Qlobal şəbəkədə böyük həcmdə pornoqrafik, insanın şərəf və ləyaqətini alçaldan, milli, dini ədavət yayan materiallar yerləşdirilir. İnternetdə müəllif hüquqlarının pozulması, məxfi informasiyadan qanunsuz istifadə halları da kütləvi şəkil alıb. Dövlətin milli təhlükəsizliyinə xələl gətirən İnternet materialları da böyük narahatlıq doğurur.

Ona görə də İnternetin tənzimlənməsi sahəsində ən mübahisəli məqamlardan biri də məhz cəmiyyətin, dövlətin və şəxsiyyətin təhlükəsizliyi ilə insan hüquqları arasındakı tarazlığın qorunub saxlanması ilə bağlıdır. İnternetdə bu təhlükəsizliyin təmin edilməsi üçün şəxsi həyatın sirlərinə dair hüquqlardan qismən imtina edilməsi tələb edilir. İnternetin təhlükəsizliyi və insan hüquqları arasındakı həmin balans daim bu və ya digər tərəfin xeyrinə dəyişir. Təhlükəsizlik məsələlərinə diqqəti artırdıqda insan hüquqlarının müdafiəsi zəifləyir. İnsan hüquqlarının çərçivəsini genişləndirdikdə isə dövlətin, cəmiyyətin maraqları təhlükə altına düşür.

Daha bir problem ondan ibarətdir ki, İnternetin sürətli inkişafı bu sahədə yaranan problemləri tənzimləmək üçün zəruri olan normativ-hüquqi aktların qəbulu prosesini xeyli qabaqlayır. Ona görə də İnternetin tənzimlənməsi sahəsində həllini gözləyən ən mühüm problemlərdən biri də məhz baş verən texnoloji yeniliklərə qanunvericilik

sistemlərinin çevik, adekvat reaksiya vermələrinin hüquqi mexanizmlərini işləyib hazırlamaqdır.

Beləliklə, yuxarıda qeyd edilən məsələlər İnternetin tənzimlənməsi zərurətini aktual məsələ kimi ortaya qoyur. Son vaxtlar aidiyyəti beynəlxalq təşkilatlarda, dünyanin müvafiq qabaqcıl elmi, siyasi və digər tədqiqat mərkəzlərində mütəxəssislər tərəfindən bu problem ciddi şəkildə araşdırılır, müxtəlif həll yolları təklif edilir.

Oxuculara təqdim edilən bu tədqiqat işində də İnternetin tənzimlənmsinə dair beynəlxaq təşəbbüslər, bu qlobal şəbəkənin tənzimlənməsi üçün beynəlxalq miqyasda tətbiq edilən metodlar və hüquqi mexanizmlər, eləcə də İnternetdəki fəaliyyətlə bağlı yurisdiksiyanın müəyyən edilməsi, şəxsi həyatın toxunulmazlığı və fərdi məlumatların qorunması, domen adları sisteminin idarə edilməsi, İnternet-provayderlərin hüquqi məsuliyyətinin müəyyənləşdirilməsi, kibercinayətkarıqla, spamlarla mübarizə, intellektual mülkiyyət hüquqlarının qorunması, elektron kommersiya fəaliyyətinin tənzimlənməsi kimi qlobal şəbəkənin normal fəaliyyəti və inkişafı üçün mühüm əhəmiyyət kəsb edən məsələlər araşdırılır. Bu sahədə beynəlxalq və regional təşkilatların, habelə qabaqcıl ölkələrin təcrübəsi öyrənilir və analiz edilir.

1. İNTERNETİN TƏNZİMLƏNMƏSİNƏ DAİR BEYNƏLXALQ TƏŞƏBBÜSLƏR

İnternetin heyrətamiz xüsusiyyətlərindən biri də onun yaradıldığı dövrdə və ilkin inkişaf mərhələsində unikal idarəetmə sisteminin olması idi. İnternet dövlət layihəsi kimi fəaliyyətə başladı. 1960-cı illərin sonlarında ABŞ hökuməti Qabaqcıl Müdafiə Tədqiqat Layihələri Agentliyinin (*Defense Advanced Research Projects Agency - DARPA*) fəaliyyətini maliyyələşdirdi. Burada məqsəd hətta atom zərbəsi zamanı fəaliyyət göstərməyə qadir olan şəbəkə yaratmaq idi. Bunun nəticəsində də Qabaqcıl Tədqiqat Layihələri Agentliyi Şəbəkəsi (*Advanced Research Projects Agency Network - ARPANET*) meydana gəldi [2].

1980-ci ildən başlayaraq artıq İnternet adlanan bu şəbəkənin imkanlarından daha geniş beynəlxalq ictimaiyyət istifadə etməyə başladı. 1986-cı ildə İnternetin layihələndirilməsi üzrə İşçi Qrupu (*Internet Engineering Task Force – IETF*) yaradıldı. *IETF* geniş iştirakçı dairəsini cəlb etməklə əməkdaşlıq və konsensus əsasında qərarlar qəbul edərək, İnternetin sonrakı inkişafını idarə edirdi. İlkin dövrlərdə İnternetin mərkəzi hakimiyyəti, mərkəzləşdirilmiş planlaşdırılması, uzunmüddətli strategiyası yox idi.

Həmin vaxtlar vəziyyət çox sadə idi. Lakin 1994-cü ildə ABŞ Milli Elm Fondu İnternetin fəaliyyətinin təmin edilməsinə özəl sektoru da cəlb etmək qərarına gəldi və domen adları sisteminin (*Domain Name System - DNS*) idarə edilməsini *Network Solutions Inc. (NSI)* şirkətinə həvalə etdi. İnternet ictimaiyyəti bu addıma mənfi reaksiya verdi və "*DNS* müharibəsi" başlandı.

Həmin "*DNS* müharibəsi" digər iştirakçıları: biznesi, beynəlxalq təşkilatları və dövləti də İnternetin tənzimlənməsinə cəlb etdi. Bu müharibə 1998-ci ildə yeni təşkilatın – İnternetdə adların və nömrələrin verilməsi üzrə Korporasiyanın (*Internet Corporation for Assigned Names and Numbers - ICANN*) yaranması ilə nəticələndi.

ICANN-ın yarandığı ildən – 1998-ci ildən başlayaraq İnternetin idarə edilməsi məsələləri üzrə disskussiyalara BMT strukturları vasitəsilə milli hökumətlər də fəal surətdə qoşulmağa başladı.

1998-ci ildə ABŞ hökuməti tərəfindən hazırlanmış İnternetin idarə edilməsinə dair "Ağ kitab" *ICANN*-ın yaradılması ilə bağlı aşağıdakı rəhbər prinsipləri müəyyən edir [3]:

- *Stabillik*: İnternetin fəaliyyəti pozulmamalıdır, xüsusilə bu, "əsas" serverlər də daxil olmaqla, onun əsas strukturlarının işinə aiddir.
- *Rəqabət*: yaradıcı yanaşmanı və çevikliyi dəstəkləmək vacibdir, çünki bu, İnternetin daha da inkişaf etməsinə imkan verəcək.
- *Qərarların qəbulu*: yeni sistem İnternetin əvvəlcədən müəyyən edilmiş bir sıra qayda və prinsiplərini ("aşağıdan" təşkil etməni, açıqlığı və s.) özündə əks etdirməlidir.
- *Təmsilçilik*: yeni struktura bütün maraqlı tərəflər (coğrafi (müxtəlif ölkələr) və peşə (müxtəlif peşə cəmiyyətləri) baxımından) daxil edilməlidir.

ICANN-ın İnternetin idarə edilməsindəki roluna dair ziddiyyətli baxışlar mövcuddur [4]. Bu məsələdə dar-texniki və geniş-siyasi baxışlar üstünlük təşkil edir. Dar-texniki yanaşmaya görə, *ICANN* yalnız İP ünvanları və domen adları sahəsində texniki inzibatçılığı həyata keçirən

əlaqələndirici orqandır. Bu nöqteyi-nəzərdən, *ICANN* İnterneti idarə etmir, yalnız koordinasiya edir. Bu mövqeyi *ICANN,* ABŞ hökuməti, digər bəzi inkişaf etmiş ölkələr dəstəkləyirlər.

Geniş-siyasi yanaşmaya görə, *ICANN*-ın fəaliyyətinə yalnız texniki koordinasiya deyil, daha çox məsələlər daxildir. Bu yanaşmanın tərəfdarları hesab edirlər ki, *ICANN*-ın "köklü" serverlərin idarə edilməsi və İP ünvanlarının paylanması kimi əsas texniki funksiyalarının saxlanması zəruri olsa da, İnternetin idarə olunması üzrə siyasət bütün dövlətlərin təmsil olunduğu legitim beynəlxalq təşkilat tərəfindən hazırlanmalıdır. Bu isə BMT və ya xüsusi olaraq yaradılan beynəlxalq struktur vasitəsi ilə həyata keçirilə bilər. Belə bir mövqeni, əsasən, inkişaf etməkdə olan ölkələr dəstəkləyir.

Həmçinin son vaxtlar Avropa Birliyi də İnternetin idarə edilməsində *ICANN*-ın inhisarçı roluna qarşı çıxır [6]. Son vaxtlar bu təşkilat *ICANN*-ın beynəlxalq nəzarətə verilməsinə cəhd göstərir. *ICANN*-ın statusunun dəyişdirilməsi cəhdlərinin səbəbi milli əlifbalarda domen zonalarının yaradılması ideyası ilə bağlıdır.

2009-cu ilin iyun ayının 19-da Avropa Birliyi Komissiyasının dərc etdiyi strateji sənəddə domen zonalarının baş administratorunu (*ICANN*-ı) dəyişməyə çağırırdı [7]. Sənəddə birbaşa qeyd olunurdu ki, *ICANN*-ın texniki fəaliyyətinə dair heç bir irad yoxdur, lakin bütün dünya domen infrastrukturuna görə məsuliyyət daşıyan bu təşkilatın Kaliforniya qanunları ilə fəaliyyət göstərməsi, yalnız ABŞ hakimiyyəti qarşısında hesabatlı olması Avropa üçün qəbulolunmazdır.

Müşahidələr və təhlillər göstərir ki, bu cür sənədlər rəsmi Vaşinqtonun domen sistemi üzərində nəzarətdən

məhrum etmək məqsədi daşıyır. Çünki *ICANN*-ın ABŞ-ın Ticarət Nazirliyi ilə növbəti müqaviləsinin müddəti 2009-cu ilin sentyabr ayında başa çatırdı. Ona görə də domen sisteminin administratorunun dəyişməsində maraqlı olanlar əvvəlcədən bu prosesə hazırlaşırdılar. Bir sıra ölkələr isə domenlərin baş qeydiyyatçısının funksiyasını BMT yanında yaradılan yeni beynəlxalq təşkilata verilməsini təklif edirdilər.

Lakin narazı qüvvələr öz məqsədlərinə yalnız qismən nail ola bildilər. Belə ki, 2009-cu ilin sentyabr ayının 30-da İnternetin idarə edilməsi ilə bağlı *ICANN*-la ABŞ-ın Ticarət Nazirliyi arasında bağlanmış müqavilənin müddəti başa çatsa da, Avropa Birliyinin tələblərinə baxmayaraq, *ICANN* ABŞ Konqresinə göndərdiyi məktubunda bu ölkə ilə uzunmüddətli əlaqələri saxlamaqda maraqlı olduğunu bəyan etdi [3]. Bu istəyə uyğun olaraq, sentyabrın 30-da *ICANN*-la ABŞ-ın Ticarət Nazirliyi arasında İnternetin fəaliyyətinin idarə edilməsi ilə bağlı yeni müqavilə imzalandı. Bu müqavilə artıq oktyabr 2009-cu il tarixindən qüvvədədir. Həmin sənəddə bu tərəflər arasında bağlanmış əvvəlki müqavilədə öz əksini tapan ABŞ dövlətinin *DNS* sisteminin idarəçiliyinin *ICANN*-a verilməsinə dair, həmçinin İnternetin fəaliyyətinin idarə olunması ilə bağlı öhdəliklər bir daha təsdiq edilir.

Ekspertlərin fikrincə, yeni razılaşma İnterneti daha da beynəlmiləlləşdirəcək. Belə ki, bu müqavilədə İnternetin fəaliyyəti ilə əlaqədar beynəlxalq təmsilçilərin iştirakı ilə bir neçə nəzarət şurasının yaradılması nəzərdə tutulur [8]. ABŞ dövləti əvvəlki kimi *ICANN*-a göstərişlər verə biləcək, lakin artıq bu göstərişlər hüquqi qüvvəyə malik olmayacaq. Əvvəlkindən fərqli olaraq, yeni müqavilə qeyri-müəyyən müddət üçün imzalanıb. Ekspertlər hesab

edirlər ki, bu da ABŞ dövlətinin *ICANN*-nın fəaliyyətinin nəticələrinə əvvəlki kimi nəzarət etmək imkanını aradan qaldırır.

Yeni müqaviləyə əsasən, ICANN ildə 1 dəfədən az olmayaraq yalnız ABŞ dövləti qarşısında deyil, həm də bu təşkilatda təmsil olunan bütün strukturlar, o cümlədən 80-dən çox ölkənin təmsil olunduğu Dövlət Nümayəndələrinin Məşvərət Komitəsi (*GAC*) qarşısında hesabat verməlidir [3]. Bundan başqa, *ICANN*-nın fəaliyyətinə xüsusi təftiş komissiyası tərəfindən nəzarət ediləcək. Həmin komissiya 3 ildə 1 dəfə ICANN-nın İnternetin idarə edilməsi üzrə öz vəzifələrini necə yerinə yetirməsinə dair tam hesabat verməlidir. Müvafiq komissiyanın üzvləri *ICANN*-ın prezidenti və *GAC* sədri tərəfindən təyin olunurlar.

İnternetin beynəlxalq səviyyədə tənzimlənməsi məsələsi informasiya cəmiyyəti məsələlərinə həsr olunan beynəlxalq toplantıların da əsas müzakirə obyektlərindən biridir. 2003-cü ilin dekabrında Cenevrədə keçirilən informasiya cəmiyyəti üzrə Ümumdünya Sammitinin (İCÜS) gündəliyinə İnternetin idarə edilməsi məsələsi də daxil edilmişdi. İCÜS tərəfindən qəbul edilmiş Prinsiplər Bəyannaməsində və Fəaliyyət Planında İnternetin idarə edilməsi sahəsində bir sıra tədbirlər, o cümlədən İnternetin idarə edilməsi üzrə İşçi Qrupunun (*Working Group on Internet Governance – WGIG*) yaradılması təklif olundu [5].

İCÜS-ün Prinsiplər Bəyannaməsinin İnternetin idarə olunması ilə bağlı 50-ci maddəsində qeyd edilir: "Beynəlxalq səviyyədə İnternetdən istifadənin idarə edilməsi məsələləri razılaşdırılmış qaydada həll edilməlidir. Biz BMT-nin Baş katibinə 2005-ci ilə qədər

İnternetdən istifadənin idarə edilməsi ilə əlaqədar məsələlərin öyrənilməsi və lazımi hallarda qərarların qəbul edilməsi üçün təkliflərin verilməsi məqsədilə istər inkişaf etməkdə olan, istərsə də inkişaf etmiş ölkələrdə, o cümlədən müvafiq hökumətlərarası və beynəlxalq təşkilatlarda, forumlarda dövlət idarəetmə orqanlarının, özəl sektorun və vətəndaş cəmiyyətinin geniş miqyaslı və fəal iştirak mexanizmini təmin edən açıq və hər şeyi əhatə edən proses çərçivəsində İnternetdən istifadənin idarə edilməsi üzrə işçi qrupunu təsis etmək barədə müraciət edirik".

İCÜS-ün İnternetin idarə edilməsinə həsr edilən fəaliyyət planı maddəsində də (13.b.) yuxarıdakı müddəalar öz əksini tapmışdı [5]. Həmin işçi qrupunun qarşısında aşağıdakı məsələlər qoyulurdu:

- İnternetdən istifadənin idarə edilməsinin işçi tərifini işləyib hazırlamaq;
- İnternetdən istifadənin idarə edilməsinə aid olan dövlət siyasəti ilə bağlı problemləri üzə çıxartmaq;
- inkişaf etməkdə olan və inkişaf etmiş ölkələrin dövlət idarəetmə orqanlarının, mövcud dövlətlərarası və beynəlxalq təşkilatların və digər forumların, habelə özəl sektorun və vətəndaş cəmiyyətinin rolunu müəyyən etmək;
- 2005-ci ildə Tunisdə İnformasiya cəmiyyəti məsələləri üzrə Ümumdünya Sammitinin 2-ci mərhələsinin gedişində müzakirəyə təqdim etmək və müvafiq qərarın qəbul edilməsi üçün görülən işlərin nəticələri barədə hesabat hazırlamaq.

Beləliklə, İnternetin beynəlxalq səviyyədə tənzimlənməsi məsələsi ilk dəfə BMT-nin Baş Katibliyi yanında 2004-2005-ci illərdə fəaliyyət göstərən "İnternetin idarə edilməsi üzrə İşçi Qrupu"nun yaradılması prosesində qoyuldu.

WGIG öz fəaliyyəti müddətində Cenevrədə dörd iclas keçirdi: 2004-cü ilin 23-25 noyabrında, 2005-ci ilin 14-18 fevralında, 2005-ci ilin 18-20 aprelində və 2005-ci ilin 14-17 noyabrında [9].

WGIG müəyyən edilən meyarları, təhlil və təklifləri, həmçinin maraqlı tərəflər arasında aparılan geniş disskussiyaları nəzərə alaraq, İnternetin idarə edilməsinin işçi tərifini verdi: "İnternetin idarə edilməsi hökumət, özəl sektor və vətəndaş cəmiyyətinin öz funksiyalarını yerinə yetirərkən onlar tərəfindən İnternetin təkamülünü və tətbiqini tənzimləyən ümumi prinsiplərin, normaların, qaydaların, qərarların və proqramların qəbul olunma prosedurlarının işlənib hazırlanmasını və tətbiq edilməsini özündə əks etdirir."

Bu işçi tərif dövlətlərin, özəl sektorun və vətəndaş cəmiyyətinin İnternetin idarə olunması mexanizmlərində geniş iştirak konsepsiyasını möhkəmləndirir. Həmçinin təsdiq edir ki, İnternetin idarə edilməsinə dair konkret məsələyə yanaşmada hər bir qrupun öz maraqları, funksiyaları var.

Lakin İnternetin idarə edilməsi yalnız İnternet adlarını və ünvanlarını deyil, həmçinin *ICANN*-ın məşğul olduğu məsələləri, dövlət siyasətinin digər mühüm problemlərini - İnternet resurslarını, onun təhlükəsizliyini, istifadə və inkişaf məsələlərini əhatə edir.

İşçi Qrupunun fəaliyyətinin nəticəsi kimi Yekun sənədi qəbul edildi [10]. Yekun sənədində müvafiq

problem üzərində işlərin təşkili üzrə bir sıra prinsipial təkliflər öz əksini tapdı. İşçi Qrupunun yekun sənədində İnternetin tənzimlənməsində maraqlı olan tərəflərin – dövlətin, özəl sektorun və vətəndaş cəmiyyətinin hər birinin üzərinə müəyyən vəzifələr qoyulur.

Dövlətin üzərinə qoyulan vəzifələr aşağıdakılar idi:

- milli səviyyədə müvafiq dövlət siyasətinin hazırlanması, koordinasiyası və həyata keçirilməsi;
- İKT-nin inkişafı üçün əlverişli şəraitin yaradılması;
- nəzarət funksiyasının yerinə yetirilməsi;
- qanunların, əsasnamələrin və standartların işlənməsi və qəbul edilməsi;
- müqavilələrin işlənib hazırlanması;
- qabaqcıl təcrübənin inkişaf etdirilməsi;
- texnologiya və standartlar sahəsində elmi tədqiqatların və təcrübə-konstruktor işlərinin həvəsləndirilməsi;
- İKT sahəsindəki xidmətlərin əlyetərliliyinin stimullaşdırılması;
- kibercinayətkarlığa qarşı mübarizə;
- beynəlxalq və regional əməkdaşlıq;
- İKT infrastrukturunun inkişafının və yeni tətbiqi proqramların yaradılmasının həvəsləndirilməsi;
- ümumi inkişaf problemlərinin həll edilməsi;
- çoxdilliliyin və mədəni müxtəlifliyin həvəsləndirilməsi;
- mübahisələrin və arbitrajların tənzimlənməsi.

Özəl sektorun üzərinə də bir sıra vəzifələr qoyulurdu:

- informasiya sənayesində özünütənzimləmənin həyata keçirilməsi;
- qabaqcıl təcrübənin inkişaf etdirilməsi;
- rəhbər orqanlar və digər maraqlı tərəflər üçün strateji təkliflərin, rəhbər prinsiplərin və metodların işlənib hazırlanması;
- texnologiyalar, standartlar və proseslər sahəsində elmi tədqiqatların və təcrübə-konstruktor işlərinin aparılması;
- milli qanunvericiliyin, milli və beynəlxalq siyasətin hazırlanmasında iştirak;
- innovasiya fəaliyyətinin həyata keçirilməsi;
- arbitraj və mübahisələrin tənzimlənməsi;
- potensialın artırılmasının stimullaşdırılması.

Vətəndaş cəmiyyətinin üzərinə qoyulan vəzifələr də vardı:

- cəmiyyətin informasiyalılığının genişləndirilməsi və potensialın yaradılması (biliklər, kadrların hazırlanması, təcrübə mübadiləsi);
- dövlət maraqlarına cavab verən müxtəlif hədəflərə çatmaq üçün fəaliyyət göstərilməsi;
- sosial şəbəkələrin yaradılması;
- demokratik proseslərin gedişində vətəndaşların qloballaşdırılması;
- əhalinin marginal qruplarının problemlərinin həlli;
- siyasi proseslərdə iştirak;
- İKT sahəsində siyasi istiqamətlər üzrə ekspertlərin, mütəxəssislərin, təcrübə və biliklərin təqdim edilməsi;

- texnologiyalar və standartlar sahəsində elmi tədqiqatların və təcrübə-konstruktor işlərinin aparılması;
- qabaqcıl təcrübənin inkişaf etdirilməsi və yayılması;
- insan hüquqları, dayanıqlı inkişaf, sosial ədalət və geniş imkanların yaradılması əsasında şəxsiyyətyönümlü informasiya cəmiyyəti konsepsiyasının formalaşdırılması istiqamətində fəaliyyət göstərilməsi.

İşçi Qrupun yekun sənədində ən mühüm məqam isə İnternetin idarə edilməsi üzrə Qlobal Forumun təşkil edilməsinin qərara alınması idi. Beləliklə, 2006-cı ildə BMT tərəfindən İnternetin idarə edilməsi üzrə Forum (*Internet Governance Forum - İGF*) təsis edildi. Bu qurum İnternetin idarə edilməsi üzrə İşçi Qrupunu əvəz etdi.

Forumun əsas vəzifəsi İnternetin səmərəli fəaliyyətini, etibarlı istismarını, təhlükəsizliyini, stabilliyini və inkişafını təmin etmək məqsədilə bu qlobal şəbəkədən istifadənin idarə olunmasının əsas elementlərinə dair dövlət siyasətini müzakirə etməkdir.

BMT-nin Baş katibi Pan Qi Mun Forumun əhəmiyyəti barədə bunları qeyd etmişdir: "Bu Forumun fərqləndirici cəhəti burada bir çox maraqlı tərəflərin informasiya və qabaqcıl təcrübə mübadiləsi əsasında qarşılıqlı fəaliyyət göstərmələridir. Bundan başqa, bu Forum İnformasiya cəmiyyətinə həsr olunmuş Tunis Sammitinin yekun sənədlərində göstərildiyi kimi, dövlətlərə, özəl sektora və vətəndaş cəmiyyətinə dayanıqlı, fasiləsiz fəaliyyət göstərən təhlükəsiz və stabil İnternetin formalaşması üçün birgə fəaliyyət göstərmək imkanı verir" [11].

İndiyə kimi bu Forumun 4 iclası keçirilib [12]:

1. Afina (Yunanıstan), 30 oktyabr - 2 noyabr 2006-cı il.
2. Rio-de-Janeyro (Braziliya), 12-15 noyabr 2007-ci il.
3. Heydərabad (Hindistan), 3-6 dekabr 2008-ci il.
4. Şarm-əl-Şeyx (Misir), 15-18 noyabr 2009-cu il.

Forumun növbəti iclasının 2010-cu ildə Vülnüsdə (Litva) keçirilməsi nəzərdə tutulur [3].

İGF-in Yunanıstan paytaxtında keçirilən ilk toplantısında əsas diqqət İnternetin inkişafının dörd mühüm aspektinə - təhlükəsizlik, müxtəliflik, açıqlıq və əlyetərliliyə yönəldildi. Bundan başqa, Forumda bir çox ölkələr üçün əhəmiyyətli olan domen adları ilə bağlı məsələlər də geniş müzakirə olundu.

Forumun Rio-de-Janeyro şəhərində keçirilən ikinci iclasının gündəliyinə də İnternet-resurslar, əlyetərlilik, müxtəliflik, açıqlıq, təhlükəsizlik kimi məsələlərin müzakirəsi daxil edilmişdi.

Forumun 3-cü iclasının gündəliyində əlyetərlilik, çoxdillilik, kibertəhlükəsizlik və etimad, kibercinayətkarlıq, şəxsi həyatın toxunulmazlığı, şəffaflıq, əsas İnternet resurslarının idarə edilməsi, qlobal, regional və milli tənzimləmə, habelə innovativ inkişaf məsələləri var idi.

İclasın yekun sənədində şəxsi həyatın təhlükəsizliyi və toxunulmazlığı ilə bağlı dövlətlərə aşağıdakı tədbirlərin görülməsinə dair tövsiyələr irəli sürülür:

- cəmiyyətin kibercinayətkarlıqdan qorunmasına yönələn məsələlərə dair ümumi siyasətin hazırlanması;

- şəbəkə və informasiya təhlükəsizliyinin gücləndirilməsi;
- spamla mübarizə üzrə qanunların qəbulu və səlahiyyətli orqanların yaradılması;
- İnternet-provayderlərlə hüquq-mühafizə orqanları arasında əməkdaşlığa dair ümumi normaların işlənib hazırlanması;
- fərdi məlumatların və şəxsi həyatın toxunulmazlığının qorunması;
- müəllif və əlaqəli hüquqlar sahəsində piratçılıqla mübarizə aparılması;
- elektron kommersiyanın effektli fəaliyyətini təmin etmək məqsədilə işgüzar sektor və istehlakçılar arasında qarşılıqlı əlaqələrin gücləndirilməsi;
- uşaqların İKT və İnternetdən daha təhlükəsiz istifadəsinin təmin edilməsi;
- cəmiyyətin İnternetdən istifadəsinə və kontentlərin yaradılmasında fəallıq göstərməsinə nail olmaq;
- sərhədlərdən asılı olmayaraq İnternetdə ünsiyyət və yaradıcılıq azadlığını genişləndirmək;
- bütün vətəndaşların dövlət idarəetməsində iştirakını təmin etmək məqsədilə onların İnternet vasitəsilə açıq dövlət informasiya resurslarına daxil olmalarına nail olmaq.

Üçüncü Forumda müzakirə edilən əsas məsələlərdən biri də İnternet istifadəçilərinin sayının artırılması ilə bağlı idi. Bu məqsədə çatmağın mümkün yolları kimi İnternetdə çoxdilliliyin inkişaf etdirilməsi və əlyetərliliyin

genişləndirilməsi göstərildi. Öz növbəsində, çoxdilliliyin inkişaf etdirilməsinin əsas yolu kimi milli əlifba simvollarından istifadə etməklə domen adlarının yaradılmasının zəruriliyi qeyd edildi.

Kibertəhlükəsizliyin təmin edilməsində əsas hüquqi problem kimi yurisdiksiya və coğrafi sərhədlər, həmçinin qanunvericilik vasitələrinin sürətlə dəyişən texnoloji situasiyaya ləng adaptasiyası qeyd edildi.

Forumun Misirin Şarm-əl-Şeyx şəhərində keçirilən sonuncu iclasının gündəliyinə aşağıdakı məsələlər daxil edilmişdi:

- İnternet resurslarının idarə edilməsi;
- İnternetdə təhlükəsizlik, açıqlıq və konfidensiallıq siyasətinin həyata keçirilməsi;
- İnternetə müxtəlif çıxış imkanlarının təmin edilməsi;
- İnternetin İnformasiya cəmiyyətinin inkişafı məsələlərinə həsr olunmuş Cenevrə və Tunis Sammitlərinin prinsiplərinə uyğun idarə edilməsi;
- Yeni çağırışlar və yeni imkanlar: sosial şəbəkələrin İnternetə təsiri.

Forumun iclas və seminarlarının gedişində həmçinin İnternetin hüquqi tənzimlənməsi, İnternetdə uşaqların müdafiəsi, *ICANN*-ın fəaliyyəti, milli domenlərin idarə edilməsi kimi məsələlərə də baxılıb.

Ümumiyyətlə, qeyd etmək lazımdır ki, *İGF* beynəlxalq səviyyədə prinsipial qərarların qəbul olunduğu meydan deyil. *İGF* yalnız əsas tendensiyaların müəyyən edilməsi üçün müsbət təcrübənin və nailiyyətlərin mübadilə meydanıdır.

Bu günkü situasiya göstərir ki, İnternetin idarə edilməsinin beynəlmiləlləşdirilməsi üzrə danışıqlar prosesinə qədərki aralıq mərhələ kimi nəzərdə tutulan bu Forum onu yaradanların ümidlərini doğrultmayıb. Belə ki, Forum İnternetə nəzarətin beynəlxalq ictimaiyyətə ötürülməsi məsələsinə lazımi diqqət yetirmir. Problemi müzakirə edənlərin əhatə dairəsinin olduqca geniş (dövlət, biznes və vətəndaş cəmiyyəti nümayəndələrindən ibarət), danışıqların formatının açıq olması konstruktiv dialoqa mane olur.

ABŞ yaranmış vəziyyətə öz milli maraqları prizmasından yanaşır və İnternetin ad və ünvan məkanı üzərində nəzarəti əldən vermək fikrində deyil. Lakin inkişaf etməkdə olan və bir sıra inkişaf etmiş ölkələr tərəfindən dəstəklənən Beynəlxalq Telekommunikasiya İttifaqının (BTİ) mövqeyi də olduqca sərtddir. BTİ-nin Baş katibi H.Turc çıxışlarının birində qeyd etmişdir ki, əgər *İGF*-in fəaliyyətinin gedişində İnternetin idarə edilməsi vəziyyətini dəyişmək mümkün olmasa, müzakirə yerini dəyişmək və müvafiq problemlərin BTİ-nin səlahiyyətli konfransları çərçivəsində həllinə cəhd etmək lazım gələcək. Qeyd edək ki, BTİ-nin növbəti konfransı 2010-cu ildə keçiriləcək.

2. İNTERNETİN TƏNZİMLƏNMƏSİ ÜSULLARI

İnternetin beynəlxalq səviyyədə tənzimlənməsi üçün ən vacib məsələlərdən biri bütün maraqlı tərəfləri təmin edən optimal üsulların seçilməsidir.

Tənzimləmə üsulları – tənzimləyən subyektin müəyyən məqsədlərə çatmaq üçün tənzimlənən subyektə göstərdiyi təsir metodları və vasitələrinin məcmusudur. Tənzimləmənin təşkilati-hüquqi, iqtisadi və sosial-psixoloji üsulları mövcuddur.

İnternetin tənzimlənməsinə dair beynəlxalq praktikada müəyyən üsullar tətbiq edilir ki, bunlar da, əsasən, təşkilati-hüquqi xarakterlidir. Bu üsulları aşağıdakı kimi təsnif etmək olar [5]:

- yanaşmalar;
- rəhbər prinsiplər;
- analogiyalar.

İnternetin tənzimlənməsi prosesinin özü kimi, bu üsullar da daim dəyişir. Yanaşmalar, modellər, rəhbər prinsiplər və analogiyalar onların hazırkı beynəlxalq danışıqlar prosesi üçün uyğunluğundan və zəruriliyindən asılı olaraq yaranır və yox olur.

Yanaşmalar

İnternetin tənzimlənməsi ilə bağlı beynəlxalq praktikada başlıca olaraq iki yanaşma mövcuddur: **"dar" və "geniş" yanaşma** [5]. İndiyə kimi İnternetin tənzimlənməsi ilə bağlı beynəlxalq danışıqlar prosesində müxtəlif maraqları əks etdirən "dar" və "geniş" yanaşmalar arasındakı qarşıdurma əsas problemlərdən biri olaraq qalır.

"Dar" yanaşma zamanı, ilk növbədə, İnternetin infrastrukturuna (domen adları sisteminə, İP ünvanlarına və "köklü" serverlərə) və bu meydanda əsas oyuncu olan *İCANN*-ın mövqeyinə diqqət yetirilir.

"Geniş" yanaşmaya uyğun olaraq, İnternetin idarə edilməsi üzrə danışıqlar infrastruktur məsələlərinin hüdudlarından kənara çıxır və digər problemlərə (hüquqi, iqtisadi, sosial-mədəni, inkişaf məsələləri ilə bağlı) diqqət yetirilir. Bu yanaşma İnternetin tənzimlənməsi məsələlərinə dair siyasi və elmi disskussiyalarda da üstünlük təşkil edir.

Artıq disskussiyalarda bu yanaşmalardan hansının doğru olmasından söhbət getmir. İndi beynəlxalq danışıqlar "dar" (*İCANN*-la bağlı olan məsələlər) və "geniş" (İnternetin idarə edilməsinin digər aspektləri) yanaşmalar arasında daha münasib balansın yaradılması mərhələsinə keçib.

Texniki və siyasi aspektlər İnternetin tənzimlənməsi məsələsində mühüm yanaşma kimi çıxış edir. Bu aspektlərin inteqrasiyası İnternetin idarə edilməsi nöqteyi-nəzərincə ciddi siqnaldır. Çünki bu aspektlər arasında dəqiq sərhəd çəkmək qeyri-mümkündür. Texniki qərarlar neytrallığı əks etdirmir. Yəni son nəticədə istənilən texniki qərar hansısa maraqlara xidmət edir, müəyyən qrupların mövqelərini gücləndirir və aşkar şəkildə ictimai, siyasi və iqtisadi proseslərə təsir edir.

Belə hallar məlumdur ki, texniki qərarı müəyyən edən ilkin siyasi məqsəd sonradan dəyişib. Məsələn, İnternetin verilənlərin birbaşa ötürülməsinə və paket kommutasiyasına əsaslanan arxitekturu siyasi məqsədlər üçün - nüvə zərbəsinə davam gətirən etibarlı şəbəkə yaratmaqdan ötrü qurulmuşdu. Həmin arxitektur sonradan

İnternetdə yaradıcılığın inkişafı və özünüifadə azadlığının əsasına çevrildi.

İnternetin inkişafının ilkin mərhələsində onun fəaliyyətinin istər texniki, istərsə də siyasi aspektləri uzun müddət yalnız bir sosial qrup – ixtiraçılar və istifadəçilər tərəfindən tənzimlənirdi. İnternetin yayılması və yeni maraqlı tərəflərin, ilk növbədə, biznes sektorunun və dövlətin meydana çıxması ilə əlaqədar 1990-cı illərdə texnologiya və siyasətin birliyi pozuldu. Tarazlığı bərpa etmək üçün İnternetin tənzimlənməsi sistemində islahat keçirildi (*İCANN*-ın yaradılması da daxil olmaqla). Bu problem açıq olaraq qalır və İnternetin idarə edilməsi üzrə Forum çərçivəsində potensial mübahisəli məsələlərdən biri kimi gündəlikdə durur.

"Real" və "kiber" yanaşma. İnternetin tənzimlənməsi çərçivəsində istənilən məsələyə iki cür baxmaq olar: köhnə "real" yanaşma və yeni "kiber" yanaşma.

Köhnə "real" yanaşmanın tərəfdarları göstərirlər ki, İnternet idarəetmə sahəsinə yeni heç nə gətirməyib. İnternet, tənzimləmə baxımından, öz sələflərindən – teleqrafdan, telefondan, yaxud radiodan fərqlənməyən növbəti texniki qurğudur. Məsələn, hüquqi aspekt üzrə olan disskussiyalarda bu yanaşmanın tərəfdarları göstərirlər ki, mövcud qanunlar kiçik düzəlişlər edilməklə İnternetə də tətbiq edilə bilər. Belə ki, İnternet insanlar arasındakı kommunikasiyalarla bağlıdır, bu texnologiya telefondan, yaxud teleqrafdan fərqlənmir, ona görə də istənilən digər kommunikasiya vasitəsi kimi tənzimlənə bilər. İqtisadiyyat sahəsində bu yanaşmanın tərəfdarları iddia edirlər ki, adi və e-kommersiya arasında fərq yoxdur.

Ona görə də onlar e-kommersiyanın xüsusi olaraq hüquqi tənzimlənməsinə ehtiyac olmadığını deyirlər.

Yeni "kiber" yanaşmanın tərəfdarları isə göstərirlər ki, İnternet bütün əvvəlki texnologiyalarla müqayisədə tamamilə yeni texnologiyadır. Ona görə də hesab edirlər ki, İnternet prinsipcə yeni tənzimləmə tələb edir. Bu yanaşma İnternetin fəaliyyətə başladığı ilk illərdə xüsusilə populyar idi. Hətta ümidlər var idi ki, İnternetin idarə edilməsinin yenilikçi üsulu – "hərtərəfli anlaşma və işləyən kod" (*rough consensus and running code*) – insan fəaliyyətinin digər sahələrində də model tənzimlənməyə çevrilə bilər. Yeni "kiber" yanaşmanın əsas mühakiməsi ondan ibarətdir ki, İnternet bizim sosial və siyasi gerçəkliyimizi suveren dövlətlər məkanından ayırır. Kibermәkan gerçək dünyadan fərqlənir, ona görə də başqa idarəetmə forması tələb edir.

ICANN-ın yaradılması prosesində bu yanaşmanın üstünlük təşkil etməsi aşkar şəkildə hiss olunurdu [3]. Belə ki, bu proses zamanı "real" dövlətlərin təsiri minimal idi. "Kiber" yanaşma 2002-ci ildə *ICANN*-ın islahatı nəticəsində yumşaldıldı ki, bu da dövlətlərin səlahiyyətlərini genişləndirdi və bu təşkilatı siyasi reallıqlara yaxınlaşdırdı.

"Kiber" yanaşmanın tərəfdarları hüquq sahəsinə müraciət edərək, iddia edirlər ki, yurisdiksiyaya, cinayətkarlığa və müqavilələrin bağlanmasına aid olan mövcud qanunlar İnternetə tətbiq edilə bilməz, ona görə də yeni qanunlar qəbul edilməlidir.

Hər iki yanaşmada tutarlı əsaslar olsa da, "real" hüquq həm nəzəriyyədə, həm də praktikada dominantlıq edir. Daha çox yayılmış fikrə görə, mövcud qanunvericiliyin böyük hissəsi İnternetə tətbiq edilə bilər.

Amma bəzi situasiyalarda (məsələn, əmtəə nişanlarının müdafiəsi kimi) real dünyada mövcud olan hüquq normalarında müəyyən dəyişikliklər etmədən onları kibermәkanda tətbiq etmək olmaz. Həmçinin spamlarla bağlı münasibətlər də tamamilə yeni qanunlarla tənzimlənməlidir. Real dünyada spama yaxın olan analogiya – makulatura (kütləvi reklam göndərişləri) poçtudur ki, o da qanunla qadağan edilməyib.

Rəhbər prinsiplər

İnternetin tənzimlənməsinin rəhbər prinsipləri müəyyən dəyərləri və maraqları özündə əks etdirir. Bu prinsiplərin təsdiqi İnternetin təşəkkül tapmaqda olan tənzimlənməsi rejimini təmin etməlidir. Həmin prinsiplərdən bəziləri – şəffaflıq və iştirak üçün açıqlıq İCÜS tərəfindən təsdiq edilib. Digər prinsiplər İnternetin tənzimlənməsi məsələləri üzrə disskussiyalarda hələlik açıq şəkildə tətbiq edilməyib [12].

Kompleks yanaşma prinsipi. Bu prinsip yalnız texniki deyil, həm də hüquqi, sosial, iqtisadi və İnternetin fəaliyyəti və təkamülü ilə bağlı aspektlərin inkişafına dair müzakirəsini nəzərdə tutur. Həmçinin rəqəmsal texnologiyaların (telekommunikasiya xidmətlərinin dəyişməsi də daxil olmaqla) İnternet-protokolların istifadə edilməsinə fəal şəkildə yaxınlaşmasını nəzərə almaq lazımdır.

Maraqlı tərəflər İnternetin idarə edilməsi üzrə danışıqlarda kompleks yanaşma üzərində dayanmaqla yanaşı, öz maraqları baxımından prioritet məsələləri müəyyən etməlidirlər. İnkişaf etmiş və inkişaf etməkdə olan ölkələr eyni qrupa aid deyil. Hətta inkişaf etməkdə

olan ölkələr arasında da prioritetlər, inkişaf səviyyəsi və İKT hazırlığı ilə bağlı fərqlər mövcuddur (məsələn, İKT nöqteyi-nəzərincə inkişaf etmiş ölkələr – Hindistan, Çin və Braziliya ilə az inkişaf etmiş Afrika ölkələri arasında).

İnternetin idarə edilməsində kompleks yanaşma və prioritetlərin müəyyən edilməsi maraqlı tərəflərə (istər inkişaf etmiş, istərsə də inkişaf etməkdə olan ölkələrə) müəyyən məsələlər ətrafında bir yerə toplaşmağa kömək etməlidir. Bu da daha məzmunlu və az siyasiləşmiş danışıqlara gətirməlidir. Onda maraqlı tərəflər ənənəvi güclü siyasiləşmiş "bölücü xətlərə" (məsələn, inkişaf etmiş – inkişaf etməkdə olan ölkələr, hökumət-vətəndaş cəmiyyəti) əsasən deyil, problemlər ətrafında qruplaşacaqlar.

Texnoloji neytrallıq prinsipi. Avropa Birliyində texnoloji neytrallıq prinsipi telekommunikasiya siyasətinin əsas dayaqlarından biri kimi müəyyən edilib. Texnoloji neytrallıq prinsipinin İnternetin tənzimlənməsi məsələlərinə adekvatlığı şübhə doğurmasa da, telekommunikasiya normaları sahəsindəki mövcud normalardan yenilərinə keçərkən çətinliklərin olması qaçılmazdır. Bu, artıq İnternet-telefoniya (*VoIP*) kimi sahələrdə özünü göstərir.

Stenford Universitetinin hüquq üzrə professoru, İnternetdə insan hüquqları uğrunda apardığı mübarizəyə görə tanınan Lorens Lessiq "Kod və kibermәkanın digər qanunları" kitabında texnologiya və siyasətin qarşılıqlı münasibətlərinin əsas aspektlərindən birinə diqqət yetirir: müasir cəmiyyət İnternetdən asılılığın artdığına görə qanunla deyil, proqram kodu vasitəsilə tənzimlənməyə başlayır [5]. Parlamentlərin və hökumətlərin bəzi qanunvericilik funksiyalarını *de fakto* kompyuter şirkətləri

və proqram təminatı istehsalçıları öz üzərlərinə götürüblər. Onlar proqram təminatından istifadə etməklə getdikcə İnternetdən daha çox asılı vəziyyətə düşən cəmiyyət həyatına təsir edə bilirlər. Əgər cəmiyyət kodun köməyi ilə (qanunlar vasitəsilə deyil) idarə edilərsə, bu, müasir cəmiyyətin siyasi və hüquqi təşkilatları üçün ciddi siqnal olacaq [8].

Analogiyalar

Bəzən elə hallar olur ki, müəyyən ictimai münasibətlərin tənzimlənməsi üçün qanunvericilikdə birbaşa nəzərdə tutulan hüquq normaları mövcud olmur. Bu halda oxşar münasibətləri tənzimləmək üçün nəzərdə tutulan hüquq normaları tətbiq edilir. Hüquqi dildə buna "hüquq normalarının analogiya üzrə tətbiqi" deyilir. Analogiyalar bizə yeni situasiyaları artıq məlum olanlar vasitəsilə anlamağa kömək edir. İnternetlə bağlı ictimai münasibətlərin tənzimlənməsi üçün xüsusi qanunvericilik bazasının hələ zəif olduğu indiki şəraitdə analogiyalardan geniş istifadə edilir. İnternetlə bağlı olan məhkəmə işlərinin əksəriyyəti analogiyalar vasitəsilə həll edilir [13].

Lakin İnternetin idarə edilməsində analogiyalardan istifadənin bir sıra məhdudiyyətləri var. Birincisi, İnternet müxtəlif xidmətləri: e-poçtu (telefonla analogiyalar), www "ümumdünya hörümçək torunu" (tele-radio yayımı ilə analogiyalar) və verilənlər bazasını (kitabxana ilə analogiyalar) əhatə edən geniş anlayışdır. Hər hansı bir texnologiya ilə analogiya İnternet anlayışını lazımsız olaraq sadələşdirə bilər.

İkincisi, müxtəlif telekommunikasiya və media xidmətlərinin yaxınlaşması baxımından onlar arasındakı

ənənəvi fərqlər aradan qalxır. Məsələn, İnternet-telefoniya (*VoIP*) texnologiyası tətbiq edildikdən sonra İnternetlə telefon rabitəsi arasında sərhəd çəkmək çox çətindir.

Bu məhdudiyyətlərə baxmayaraq, analogiyalar məhkəmə işlərinin həll edilməsində və İnternetin idarə edilməsi rejiminin yaradılmasında güclü və əsas təfəkkür aləti kimi çıxış edir. Daha çox istifadə edilən analogiyalar bunlardır: İnternet – telefon, İnternet-poçt və İnternet-televiziya [1].

İnternet - telefon rabitəsi analogiyası

Ümumi cəhətləri: İnternetin inkişafının ilkin mərhələlərində bu analogiyanın meydana gəlməsi telefon xətlərinin İnternetə çıxış üçün istifadə edilməsi faktı ilə bağlıdır. Telefonla İnternet (e-poçt və çat) arasında funksional oxşarlıq da mövcuddur: hər ikisi bilavasitə və şəxsi ünsiyyət vasitəsidir. Telefonla İnternet arasındakı daha sonrakı analogiya domen adları sisteminin təşkili zamanı telefon nömrələri sistemindən isitfadə imkanına diqqət yönəldir.

Fərqli cəhətləri: İnternetdə məlumatların ötürülməsi elektrik dövrəsinə deyil, paketlərdən istifadəyə əsaslanır. Telefon rabitəsindən fərqli olaraq İnternetdə xidmətlərin göstərilməsinə zəmanət vermək olmaz, yalnız söz vermək olar ki, bunun üçün bütün səylər göstəriləcək. Bu analogiya kommunikasiyaların yalnız bir cəhətini əks etdirir: e-poçtdan və ya çatdan istifadə. İnternetin tətbiqinin digər vacib üsullarının – "ümumdünya hörümçək torunun" (www), multimedianın və s. telefonla oxşarlığı yoxdur.

Bu analogiyadan İnternet materiallarının hər-hansı formada tənzimlənməsinin əleyhdarları istifadə edirlər

(əsasən, ABŞ-da). Onlarm fikrincə, əgər İnternet telefonla oxşardısa, İnternet-kommuni-kasiyanın məzmununa nəzarət edilməməlidir [1].

İnternet – poçt analogiyası

Ümumi cəhətləri: Funksiyaları, xüsusən, məlumat çatdırma baxımından. "E-poçt" adının özü bu oxşarlığı təsdiq edir.

Fərqli cəhətləri: Bu analogiya İnternet-serverlərdən yalnız birinə - e-poçta şamil edilir. Bundan başqa, poçt xidməti e-poçtla müqayisədə göndərənlə qəbul edən arasında daha mürəkkəb vasitəçilik strukturudur. Belə ki, e-poçtda vasitəçilik funksiyasını İnternet-provayder, yaxud *Yahoo* və ya *Hotmail* kimi poçt sistemləri yerinə yetirir.

ICANN-ın prezidenti Pol Tuomi poçt sistemi ilə *ICANN*-ın funksiyaları arasında bu cür analogiya aparıb: "Əgər İnterneti poçt sistemi, domen adları və İP ünvanları şəklində təsəvvür etsək, mahiyyətcə, onlar zəmanət verirlər ki, məktub zərfdə yazılmış ünvana gedib çıxacaq. Onların zərfin içində olanlarla, zərfdə göndərilənlərlə, məktubu almaq hüququna kimin malik olması, zərfin hansı müddətə ünvanına çatmalı olması, onun göndəriş haqqının nə qədər olması ilə heç bir əlaqəsi yoxdur. Bu məsələlərin heç biri *ICANN*-ın fəaliyyəti üçün əhəmiyyətli deyil. *ICANN*-ın funksiyası məktubun ünvanına çatmasını qarantiyalamaqdır" [14].

Ümumdünya Poçt Konvensiyası adi və e-poçt arasında bu analogiyanı aparır və ikincini "məlumatların ötürülməsi üçün telekommu-nikasiyalardan istifadə edən poçt xidməti" kimi müəyyən edir [15].

İraqda həlak olan bir Amerika əsgərinin ailəsi öz doğmalarmın şəxsi e-poçt məlumatlarına və bloquna (on-

layn-gündəliyinə) giriş əldə etmək üçün şəxsi məktubla e-poçt arasında analogiyaya apellyasiya etməyə cəhd göstərmişdilər [5]. Belə ki, onlar məktub və gündəlikdə olduğu kimi, e-poçt və bloqa varis olmaq istəmişdilər.

Provayderlərin çoxu məktubla e-poçt arasında analogiyaya razı olmayaraq, istifadəçi ilə məktubun sirrinin qorunmasına dair müqaviləni əsas gətirməklə kənar şəxslərə e-poçta və bloqa giriş imkanı verməkdən imtina edirlər.

İnternet – televiziya analogiyası

Ümumi cəhətləri: İlkin analogiya kompyuter və televizorun ekranlarının xarici görünüşündəki oxşarlıqla bağlıdır. Daha incə analogiya hər ikisinin geniş auditoriyaya yayımlanmaq üçün kommunikasiyalardan istifadəsinə əsaslanır.

Fərqli cəhətləri: Telefonla müqayisədə olduğu kimi, televiziya ilə müqayisədə də İnternet olduqca geniş anlayışdır. Televizya və kompyuterin ekranlarının oxşarlığı mübahisə doğurmasa da, onlar arasında mühüm struktur fərqləri mövcuddur. Televiziya informasiyanı "birindən çoxuna" prinsipi ilə ötürməyə imkan verir, İnternet isə müxtəlif kommunikasiya növlərindən ("təkbətək", "biri çoxu ilə", "çoxu çoxu ilə") istifadə etmək imkanı yaradır.

Bu analogiyadan İnternet materiallarının məzmunu üzərində daha sərt nəzarətin yaradılmasına cəhd edənlər istifadə edirlər. Onların fikrincə, İnternetin KİV kimi imkanları televiziyanın müvafiq imkanları ilə oxşar olduğu üçün İnternet üzərində sərt nəzarətin həyata keçirilməsi vacibdir. ABŞ hökuməti bu analogiyadan məşhur "Pino vətəndaş azadlıqları uğrunda Amerika birliyinə qarşı" (*Reno vs. ACLU*) işində istifadə etməyə cəhd etmişdi [5].

Bu işin səbəbi Konqres tərəfindən Kommunikasiyaların ədəb qaydalarına (etik normalara) uyğunluğu haqqında Akt (*Communications Decency Act*) idi. Bu Akt uşaqların pornoqrafik materiallara daxil olmasının qarşısını almaq üçün İnternet materiallarmın məzmununa ciddi nəzarət edilməsini nəzərdə tuturdu. Həmin vaxt məhkəmə televiziya ilə analogiyanı qəbul etməkdən imtina etdi.

3. İNTERNETİN TƏNZİMLƏNMƏSİNİN HÜQUQİ MEXANİZMLƏRİ

İstənilən idarəetmə müəyyən sistemin nizamlanmasına yönəlir. Hüquqi tənzimləmə də sosial idarəetmə vasitəsi kimi çıxış edərək, müəyyən sistemdə təmsil olunan subyektlərin qanuni maraqlarının reallaşdırılmasını təmin etməklə ictimai münasibətlərin nizamlanmasına xidmət edir [16].

Hüquqi tənzimləmə - ilk növbədə, dövlətin və cəmiyyətin normativ-hüquqi aktların hazırlanması və qəbulu üzrə faəliyyət kimi xarakterizə edilir.

Hüquqi tənzimləmə mexanizmi dedikdə, ictimai münasibətlərə təsir göstərmək üçün istifadə edilən hüquqi vasitələr sistemi başa düşülür.

İnternetin fəaliyyəti ilə əlaqədar meydana çıxan ictimai münasibətlərin effektli şəkildə tənzimlənməsi üçün bu cür mexanizmlərin seçilməsi və tətbiqi olduqca mühüm əhəmiyyət kəsb edir. Hazırda beynəlxalq praktikada İnternetin tənzimlənməsi sahəsində aşağıdakı hüquqi mexanizmlər tətbiq edilir və ya edilə bilər [17]:

- qanunvericilik normaları;
- sosial normalar (adətlər);
- özünütənzimləmə;
- məhkəmə təcrübəsi (məhkəmə qərarı);
- beynəlxalq hüquq

Qanunvericilik normaları

İnternetlə bağlı qanunvericilik fəaliyyəti tədricən fəallaşmaqdadır. Bu, əsasən, informasiya texnologiyalarının geniş yayıldığı və sosial-iqtisadi münasibətlərə böyük

təsir etdiyi ölkələrdə müşahidə edilir. Hazırda qanunvericilik fəaliyyətinin prioritet sahələri şəxsi həyatın, istifadəçilər haqqında məlumatların, əqli mülkiyyətin qorunması, vergi münasibətləri, kibercinayətkarlıqla mübarizə məsələləridir.

Lakin sosial münasibətlər olduqca çoxşaxəlidir və ona görə də müvafiq münasibətləri yalnız qanunvericilik üsulları ilə tənzimləmək mümkün deyil. Cəmiyyət öz mahiyyətinə görə dinamikdir və qanunvericilik normaları baş verən dəyişikliklərdən həmişə geridə qalır. Bu xüsusiyyət texnoloji inkişafın sosial reallıqları daha sürətlə dəyişdiyi müasir dövrdə özünü daha qabarıq şəkildə göstərir. Qanunvericilər bu dəyişikliklərə çevik reaksiya verə bilmirlər. Bəzən yeni münasibətlərə köhnəlmiş, vaxtı keçmiş qanunlar tətbiq edilir.

İnternetin tənzimlənməsində tətbiq edilən qanunvericilik normaları üç böyük qrupa bölmək olar [5]:

1. Xüsusi olaraq İnternet üçün yaradılanlar (məsələn, *İCANN*).
2. İnternet ilə bağlı olan məsələlərə tətbiq etmək üçün əhəmiyyətli dərəcədə adaptasiya tələb edənlər (məsələn, ticarət markalarının qorunması, e-kommersiya sahəsində vergi münasibətləri).
3. Əhəmiyyətli dərəcədə dəyişikliklər etmədən İnternetə tətbiq edilə bilənlər (məsələn, söz azadlığının müdafiəsi).

Sosial normalar (adətlər)

Qanun normaları kimi, sosial normalar da müəyyən davranışları nəzərdə tutur [18]. Qanunvericilik normalarından fərqli olaraq, heç bir dövlət müəssisəsi fiziki və hüquqi şəxsləri sosial normalara riayət etməyə məcbur etmək səlahiyyətinə malik deyil. Sosial normaların yerinə yetirilməsi cəmiyyət tərəfindən onun bir qrup üzvünün digərlərinə təsiri ilə təmin edilir. İnternet öz fəaliyyətinin ilkin dövrlərində praktiki olaraq yalnız "netiket" (*netiquette*) adlanan sosial normalar vasitəsilə tənzimlənirdi [5]. Bu normaları pozmağa görə əsas cəza tədbiri İnternet cəmiyyətinin digər üzvləri tərəfindən edilən təzyiq və bu cəmiyyətdən xaricetmə idi. İlkin inkişaf dövründə İnternet, əsasən, tədqiqatçı, müəllim və tələbələrdən ibarət kiçik qrup tərəfindən istifadə edilirdi və sosial normalara riayət olunurdu. İnternetin sonrakı inkişafı nəticəsində sosial xarakterli tənzimləmə öz effektini itirdi. Bu tip tənzimləmədən hələ də istifadə etmək olar, amma yalnız yaxşı inkişaf etmiş daxili əlaqələrə malik qapalı qruplar daxilində.

Özünütənzimləmə

1998-ci ildə ABŞ hökuməti tərəfindən İnternetin tənzimlənməsi məqsədilə hazırlanan "Ağ kitab"da müvafiq istiqamətdəki fəaliyyətdə özünütənzimləməyə üstünlük verilir [3]. Özünütənzimləmə müvafiq sosial normalar üçün də xarakterik olan bəzi elementləri özündə əks etdirir. Lakin təşkilatlanmamış tənzim edilən sistemlərdə mövcud olan sosial normalardan fərqli olaraq, özünütənzimləmə yaxşı düşünülmüş və təşkil edilmiş yanaşmaya əsaslanır. Özünütənzimləmə normaları, bir qayda olaraq, müəyyən davranış kodekslərində öz əksini tapır.

Özünütənzimləmə tendensiyası, xüsusən İnternet-provayderlər arasında daha yaxşı hiss olunur. Bir çox

ölkələrdə hakimiyyət İnternet materiallarına nəzarət etmək üçün provayderlərə getdikcə daha çox təzyiq göstərməyə başlayır. Provayderlər isə müəyyən davranış normalarının müəyyən edilməsi və nəticədə hakimiyyətin onların fəaliyyətinə qarışmasmın qarşısını almaq üçün daha çox özünütənzimləməyə meyil edirlər.

İctimaiyyət tərəfindən böyük maraq doğuran məsələlərin (məsələn, İnternet materiallarının məzmununa nəzarət siyasətinin) həlli üçün özünütənzimləmə faydalı normativ vasitə olsa da, bu üsul müəyyən risklərlə bağlıdır. Aydın deyil ki, provayderlər onların veb-saytlarında yerləşdirilən materialların məzmununu hansı dərəcədə tənzimləyə biləcək? Onlar səlahiyyətli hüquq institutlarının əvəzinə qərarlar qəbul edə biləcəklərmi? Provayderlər qiymətləndirə biləcəklərmi ki, hansı məzmunlu materialların veb-saytlarda yerləşdirilməsi məqsədəuyğundur? Həmçinin özünüifadəetmə azadlığı və şəxsi həyatın qorunması məsələlərinin provayderlər tərəfindən necə təmin olunacağı da sual doğurur.

Məhkəmə təcrübəsi (məhkəmə qərarları)

Bu təcrübə ABŞ-ın hüquq sisteminin mühüm elementidir [5]. İnternetin tənzimlənməsinə də ilk dəfə məhz bu hüquq sistemi çərçivəsində cəhd göstərilib. Müvafiq sistemdə məhkəmə presedentlərindən (xüsusən, İnternet kimi yeni məsələlərin tənzimlənməsində) qanunvericilik normaları qismində istifadə oluna bilər. Hakimlər hətta zəruri hüquq normalarının olmadığı halda da qərar qəbul etməli olurlar.

Hakimlərin müraciət etdikləri ilk hüquq institutu hüquqi analogiyadır, bu zaman hansısa yeni məsələ məlum

olan norma ilə uzlaşdırılır. İnternetlə bağlı olan məhkəmə işlərinin əksəriyyəti analogiyanın köməyi ilə həll edilir.

Beynəlxalq hüquq

Daha çox yayılmış rəyə görə, İnternetin qlobal xarakteri onunla bağlı beynəlxalq tənzimləmə tələb edir. Qlobal yanaşmanın zəruriliyi spamlarla, kibercinayətkarlıq və digər arzuolunmaz hallarla mübarizə sahəsində milli səviyyədə həyata keçirilən tədbirlərin lazımi effekt vermədiyi şəraitdə bir daha təsdiq edilir. Cinayətkarlıqla mübarizədə uğurlu universal rejim qismində mülki aviasiyanın tənzimlənməsi rejimini misal göstərmək olar [19]. Mülki aviasiya haqqında beynəlxalq müqavilələrin imzalanmasından sonra həmin sahədə diversiyaların və digər qanunsuz hərəkətlərin sayı kəskin şəkildə azalmağa başladı. Bunun əsas səbəblərindən biri odur ki, mülki aviasiya sahəsində formalaşdırılan vahid hüquqi məkan cinayətkarların "sakit liman" tapmalarına imkan vermir. Eyni zamanda, qlobal yanaşmanm zəruri olması o demək deyil ki, müəyyən məsələlər milli və regional səviyyələrdə həll edilə bilməz və ya edilməməlidir.

Qlobal tənzimləmə üçün ümumi konsensus tələb edilir ki, buna da yalnız uzunmüddətli danışıqlar yolu ilə nail olmaq olar. İnternetin tənzimlənməsi rejimini yaratmaq üçün müxtəlif beynəlxalq hüquqi mexanizmlərdən istifadə etmək lazımdır. Beynəlxalq Məhkəmənin Nizamnaməsinə uyğun olaraq, beynəlxalq hüquq resursları konvensiyalara, adətlərə və ümumi prinsiplərə bölünür [20]. Bundan başqa, "yümşaq hüquq"

adlanan beynəlxalq hüquq resursu da mövcuddur və onun əhəmiyyəti get-gedə artmaqdadır.

Beynəlxalq müqavilə hüququ. Hazırda bilavasitə İnternetlə bağlı məsələlərə həsr olunmuş yeganə beynəlxalq müqavilə Avropa Şurasının Kibercinayətkarlıq üzrə Konvensiyasıdır. Digər konvensiya və müqavilələr İnternetə yalnız qismən tətbiq edilə bilər. Buna nümunə kimi insan hüquqlarına dair normalar toplusunu göstərmək olar. Öz etiqadını ifadə etmək azadlığı Mülki və siyasi hüquqlar haqqında Paktın 19-cu maddəsi ilə qorunur [20]. İnternetlə bağlı digər hüquqlar (şəxsi həyatla, informasiya əldə etməklə bağlı) insan hüquqları sahəsində qlobal və regional müqavilələrlə tənzimlənir. Münaqişələrin həlli sahəsində əsas vasitələrdən biri Xarici arbitraj qərarlarının tanınması və yerinə yetirilməsi haqqında Nyu-York Konvensiyasıdır.

İnternetin tənzimlənməsi ilə bağlı üstünlük təşkil edən yanaşma müvafiq ümumi konvensiyanın yaradılmasıdır. Bəzi mütəxəssislər hesab edirlər ki, İnternetin tənzimlənməsi üçün geniş əhatəli hüquqi vasitənin yaradılmasına (məsələn, Dəniz hüququ üzrə BMT Konvensiyası kimi) ehtiyac var. Amma bu analogiya da qüsurludur, çünki dəniz hüququ üzrə danışıqlar mövcud adi hüququn sistemləşdirilməsini və dörd mövcud konvensiyanın inteqrasiyasını tələb edirdi. İnternetlə bağlı isə adi hüquq mövcud deyil [5]. Müvafiq hüquq normaları hələ tədricən formalaşır.

Adi hüquq. Adi hüququn inkişafı, adətən, böyük vaxt tələb edir. Yəni bunun üçün normaların yerinə yetirilməsinə dair müəyyən öhdəliklərin daha da möhkəmləndirilməsi lazımdır. Keçmişdə bu mümkün deyildi. Lakin İkinci dünya müharibəsindən sonra

texnologiyaların inkişafı olduqca kiçik zaman ərzində texnoloji tərəqqinin doğurduğu dərin iqtisadi və siyasi dəyişikliklərə çevik reaksiya verə bilmək üçün beynəlxalq normativ çərçivələrin işlənib hazırlanması müddətinin kəskin şəkildə qısaldılmasını tələb etməyə başladı. İnternet bunun əyani sübutudur. Bu qlobal şəbəkənin tənzimlənməsi rejiminin yaradılmasında adi hüququn dominantlıq edəcəyi az ehtimallıdır [17].

"Yumşaq hüquq". "Yumşaq hüquq" termini bəyannamə, rəhbər prinsiplər və qanun layihələri (model qanunlar) kimi müxtəlif siyasi sənədlərlə bağlı tətbiq edilir [20]. "Yumşaq hüququn" müəyyən edilməsi üçün linqivistik meyar "sərt hüquq"da (müqavilə hüququnda) işlədilən "etməlidir" əvəzinə "etməsi vacibdir" ifadəsidir. Yəni "sərt hüquq" normaları icbari xarakter daşıdığı halda, "yumşaq hüquq" normaları yalmz tövsiyə xarakterli olur.

Dövlətlər tərəfindən "yumşaq hüquq" əsasında bağlanmış müqavilələrə əməl edilməsinə dair nümunələr çoxdur. "Yumşaq hüquq"dan dövlətlər bir sıra səbəblərə görə, o cümlədən etimadın artırılması, baş verən dəyişikliklərin stimullaşdırılması, yeni hüquqi və idarəetmə mexanizmlərinin tətbiq edilməsi üçün istifadə edilir. "Yumşaq hüquq" İnternetin tənzimlənməsində məqbul hüquqi metod kimi tətbiq edilə bilər.

4. İNTERNET-YURİSDİKSİYANIN MÜƏYYƏN EDİLMƏSİ PROBLEMLƏRİ

Yurisdiksiya – müvafiq dövlət orqanlarının hüquqi mübahisələri və hüquq pozuntuları ilə bağlı işləri həll etmək üçün qanunvericilikdə müəyyən edilmiş səlahiyyətlərinin məcmusudur [13]. Başqa sözlə, yurisdiksiya - hər hansı bir şəxsin və ya digər hüquq subyektinin fəaliyyətinin qanuna uyğunluq baxımından qiymətləndirilməsini, qanun pozucularına qarşı hüquqi sanksiyaların tətbiqini nəzərdə tutur. Yurisdiksiya həll edilən məsələnin növündən və xarakterindən, ərazi mənsubiyyətindən asılı olaraq müəyyən edilir.

Yurisdiksiya həm də dünyanın coğrafi baxımdan dövlətlərə bölünməsinə əsaslanır. Hər bir dövlət öz ərazisində yurisdiksiyasını həyata keçirmək üçün suveren hüquqlara malikdir. Lakin İnternet transsərhəd münasibətlərini (qlobal sosial münasibətləri) formalaşdırır ki, bunu da ənənəvi hüquqi mexanizmlər vasitəsilə tənzimləmək qeyri-mümkündür.

Müasir beynəlxalq hüquqda müəyyən edilən digər mühüm prinsip beynəlxalq hüququn əsas prinsiplərini pozan fəaliyyətə (məsələn, soyqırımı və piratçılıq) tətbiq edilən universal yurisdiksiyadır.

Yurisdiksiya üç tərkib hissəsindən ibarətdir [13]:

5. *prosessual yurisdiksiya* (hansi məhkəmə və ya dövlət orqanı müvafiq səlahiyyətə malik olmasını müəyyən edir);
6. *maddi yurisdiksiya* (qanunların tətbiq olunması qaydasını müəyyən edir);

7. *icra yurisdiksiyası* (məhkəmə qərarlarının hansı qaydada yerinə yetirilməli olduğunu müəyyən edir).

Konkret situasiyalarda yurisdiksiyanı müəyyən etmək üçün aşağıdakı əsas prinsiplərdən istifadə edilir [13]:

- *ərazi prinsipi* – dövlətin öz ərazisindəki insanların və mülkiyyətin üzərindəki hakimiyyəti;
- *vətəndaşliq prinsipi* – vətəndaşların harada olmasından asılı olmayaraq dövlətin onlar üzərində hakimiyyəti;
- *istintaq prinsipi* – dövlətin onun ərazisində həyata keçirilən hər hansı fəaliyyət sayəsində baş verən iqtisadi və hüquqi nəticələri tənzimləmək hüququ.

Yurisdiksiya İnternetin tənzimlənməsində daha çox diqqət yetirilməli olan aspektlərdəndir. Belə ki, İnternetlə bağlı münaqişələrin, mübahisələrin sayı durmadan artır. Amma yurisdiksiya məsələsindəki qeyri-müəyyənliklər bir sıra problemlərin yaranmasına gətirib çıxardır [1]:

- dövlətin öz ərazisində sosial münasibətləri tənzimləməsi üçün öz hüquqi səlahiyyətlərini yerinə yetirməsi mümkün olmur;
- ayrı-ayrı fiziki və hüquqi şəxslər öz məhkəmə hüquqlarından istifadə edə bilmirlər.
- İnternetin hüquqi təhlükəsizliyini təmin etmək olmur;
- elektron kommersiyanın inkişafı ləngiyir;
- İnternetin hüquqi baxımdan təhlükəsiz zonalara parçalanması təhlükəsi yaranır.

Yurisdiksiyanın müəyyən edilməsi ilə bağlı problem münaqişə eksterritorial xarakterə malik olduqda (məsələn,

münaqişədə müxtəlif dövlətlərin vətəndaşları iştirak etdikdə və ya beynəlxalq tranzaksiya həyata keçirildikdə) yaranır. İnternetdə informasiya yerləşdirərkən onun hər hansı bir ölkənin qanunvericiliyini pozub-pozmadığını bilmək çox çətindir. Çünki İnternetdə yerləşdirilən istənilən material hər bir ölkədə əlyetərli olur. Bu baxımdan, demək olar ki, İnternetdə hər bir fəaliyyət növü beynəlxalq xarakterlidir və müxtəlif yurisdiksiyaların tətbiq edilməsinə səbəb ola bilər.

Yurisdiksiya problemini qabarıq şəkildə göstərən iki əyani və tez-tez istinad edilən məhkəmə işi 1996-cı ildə Almaniyada baxılan *CompuServe* şirkəti və 2001-ci ildə Fransada *Yahoo!* şirkəti ilə bağlı baxılan işlərdir [5].

Birinci işdə Almaniya məhkəməsi tələb etdi ki, ABŞ-ın *CompuServe* şirkəti pornoqrafik materiallara çıxışı bağlasın. Şirkət Almaniya qanunvericiliyinə riayət etmək üçün özünün ABŞ-dakı mərkəzi serverindən bu cür materialları silməli oldu. Nəticədə pornoqrafik materialların qanunla qadağan olunmadığı ölkələrdə də (ABŞ da daxil olmaqla) vətəndaşlar bu materiallardan istifadə etməkdən məhrum oldular. *CompuServe* şirkəti bu sahədə ən sərt normalara tabe olmalı oldu. Bu iş belə bir tendensiya yaratdı ki, İnternet ən məhdudlaşdırıcı normalara tabe olacaq.

Yahoo! şirkəti ilə bağlı işin kökündə isə nasizmi təbliğ edən materialların yayılmasını qadağan edən Fransa qanunvericiliyinin pozulması dayanırdı. Fransa qanunları vətandaşlarma nasizmi təbliğ edən *Yahoo!*-nun saytına daxil olmağı qadağan edir. Baxmayaraq ki, həmin sayt ABŞ-da fəaliyyət göstərir və bu ölkədə müvafiq materialların yerləşdirilməsi qanunidir.

"Real" hüquq prinsipləri baxımından *CompuServe* şirkətinin işi kimi məsələlərdə qeyri-adi heç nə yoxdur. Ümumiyyətlə, "real" hüquqa əsaslanan bu cür mühakimələr prinsipcə doğrudur, amma onlar ciddi praktiki çatışmazlıqlara malikdir ki, bu da mövcud qanunların İnternetə tətbiq edilməsi imkanlarını məhdudlaşdırır. Əsas problem İnternetlə əlaqədar olan məhkəmə işlərinin miqyasındadır, çünki demək olar, hər bir sayt və ya xidmət hansısa bir ölkənin yurisdiksiyası altına düşə bilər. Beləliklə, kəmiyyət aspekti (işlərin sayı) yeni həll yollarının axtarışını tələb edə bilər.

İnternetdə yurisdiksiya çoxluğu (müxtəlifliyi) probleminin həlli aşağıdakılar vasitəsilə mümkün ola bilər [5]:

- beynəlxalq xüsusi hüququ modernləşdirməklə;
- milli qanunları unifikasiya etməklə;
- arbitrajdan istifadə etməklə;
- İnternet istifadəçilərinin kimliyini və yerini müəyyən etmək üçün texniki imkanlardan (ilk növbədə, geolokasiya proqram təminatından) istifadə etməklə.

Ənənəvi mühakimə üsulu (icraatı) çərçivəsində milli məhkəmələr müəyyən edirlər ki, bu və ya digər işə baxa bilərlərmi və bu zaman hansı qanunlar tətbiq ediləcək. Prosessual və maddi yurisdiksiya məsələlərinin həlli beynəlxalq xüsusi hüquqa əsaslanır. Beynəlxalq xüsusi hüququn normaları yurisdiksiyanın müəyyən edilməsi üçün meyarları nüəyyən edir. Ənənəvi situasiyalardan fərqli olaraq, İnternetdə bu cür meyarlarm tətbiq olunması çox çətindir.

Ənənəvi yanaşma mürəkkəbliyinə, ləngliyinə və qiyməti yüksək olduğuna görə İnternetlə bağlı münaqişələrin, mübahisələrin həllində nadir hallarda tətbiq olunur.

Beynəlxalq xüsusi hüququn modernləşdirilməsi. Beynəlxalq xüsusi hüququn əsas mexanizmləri millətlərarası münasibətlərin, əsasən, qeyri-şəxsi xarakterli və qeyri-intensiv, fiziki və hüquqi şəxslərin iştirakı ilə müxtəlif yurisdiksiyaları əhatə edən işlərin sayının məhdud olduğu vaxtlarda yaradılıb. İnternetin meydana gəlməsi ilə millətlərarası əlaqələr adi hala çevrildi. Müxtəlif ölkələrin fiziki və hüquqi şəxsləri arasında ünsiyyət, mübadilə və münaqişələr İnternet meydana gələndən sonra əvvəlki dövrlərlə müqayisədə daha tez-tez müşahidə edilir.

İnternetlə əlaqədar milli yurisdiksiya məsələlərinin çevik və ucuz başa gələn prosedurla müəyyən edilməsi məqsədilə beynəlxalq xüsusi hüququn modernləşdirilməsi məqsədəuyğundur. O cümlədən müvafiq yurisdiksiyanın müəyyən edilməsi üçün sadələşdirilmiş prosedurdan istifadə edilməsi, işlərə on-layn rejimində baxılması və hüquqi konsul-tasiyaların çevikliyinin artırılması kimi məsələləri həll etmək mümkündür.

Avropa Şurasının qəbul etdiyi "Mülki və kommersiya məsələlərinə münasibətdə yurisdiksiya və məhkəmə qərarlarının məcburi icrası məsələləri üzrə Brüssel Konvensiyası" regional səviyyədə yurisdiksiya məsələsinin həlli prosedurunun sadələşdirilməsinə və elektron kommersiya münasibətlərində iştirak edən istehlakçıların maraqlarının müdafiəsinə xidmət edir [21].

Qlobal səviyyədə beynəlxalq xüsusi hüququn inkişaf problemlərini müzakirə etmək üçün əsas forum Haaqa konfransıdır [22]. Hazırda müvafiq danışıqlarda əsas rolu ABŞ oynayır. 1992-ci ildə ABŞ-da bu ölkə

məhkəmələrinin qərarlarının hər yerdə yerinə yetirilməsi vasitəsilə əqli mülkiyyətin müdafiəsinin gücləndirilməsi məqsədilə yurisdiksiya haqqında danışıqlar canlandırıldı. 1992-ci ildən etibarən İnternetin və elektron kommersiyanın inkişafı danışıqların gedişini dəyişdirdi. Artıq ABŞ-ın İnternet şirkətlərinin yurisdiksiyaların çoxluğu şəraitində fəaliyyət göstərmələri təhlükəli olmağa başladı. *CompuServe* və *Yahoo!* şirkətlərinə qarşı Almaniya və Fransa tərəfindən irəli sürülən məhkəmə iddiaları göstərdi ki, ABŞ-da yerləşdirilən İnternet materialları digər ölkələrdə məhkəmə istintaqlarına səbəb ola bilər [5].

Milli qanunların unifikasiyası. Bu proses dünya səviyyəsində vahid normalar toplusunuu yaranmasına səbəb ola bilər. Əgər bütün ölkələrdə hüquq normaları eyni cür olarsa, yurisdiksyanın müəyyən edilməsi məsələsi öz kəskinliyini azaldar. Unifikasiyaya beynəlxalq səviyyədə kifayət dərəcədə anlaşmanın olduğu - məsələn, hamılıqla yolverilməz sayılan uşaq pornoqrafiyası, piratlıq, kölələk, terrorizm və kibercinayətkarlıq kimi sahələrdə nail olmaq olar. Digər məslələlərlə (məsələn, spam və İnternetin təhlükəsizliyi ilə) bağlı da ayrı-ayrı ölkələrin mövqeləri tədricən bir-birinə yaxınlaşır. Ancaq İnternet materiallarının məzmununa nəzarət siyasəti də daxil olmaqla, bəzi sahələrdə qlobal konsensusun əldə edilməsi az ehtimallıdır.

Arbitraj. Yurisdiksiya probleminin həllində başqa bir variant arbitrajdır. Arbitraj (münsiflər məhkəməsi), adətən, ləng və mürəkkəb olan məhkəmə prosedurlarının əvəzinə istifadə edilə bilən mübahisələrin həllinin alternativ mexanizmidir [13]. Arbitraj mexanizmindən istifadə edərkən qərar mübahisə tərəflərinin seçdikləri bir

və ya bir neçə müstəqil şəxs tərəfindən qəbul edilir. Beynəlxalq kommersiya arbitrajı qədim ənənələrə malikdir. Münsiflərin təhqiqatı, adətən, tərəflərin şəxsi razılaşmalarına əsaslanır. Arbirtaj haqqında razılaşmaların bir çox variantları mövcuddur. Arbitraj tərəfindən onun keçirildiyi yer və prosedur, tətbiq ediləcək hüquq normaları və s. məsələlər həll edilir.

Arbitrajın əsas üstünlüklərindən biri onun prosedur və maddi yurisdiksiyanın seçilməsi problemini həll etməsidir. Bu və ya digər məsələləri mübahisə tərəfləri əvvəlcədən seçir. On-layn-arbitraj təkcə İnternetlə bağlı olan mübahisələrin deyil, həmçinin adi kommersiya anlaşılmazlıqlarının həllində istifadə edilir. Bu arbitraj forması, şahid ifadələri və qərar çıxarma da daxil olmaqla, tamamilə İnternetdə həyata keçirilir.

Arbitraj İnternetlə bağlı ən mürəkkəb məhkəmə işləri ilə əlaqədar qərarların yerinə yetirilməsində də xüsusi üstünlüklərə malikdir. Belə ki, arbitraj qərarlarının yerinə yetirilməsi ölkələrin əksəriyyəti tərəfindən imzalanan, xarici arbitraj qərarlarının tanınması və yerinə yetirilməsinə dair Nyu-York Konvensiyası ilə tənzimlənir [23]. Həmin Konvensiyaya uyğun olaraq, milli məhkəmələr arbitraj qərarlarını yerinə yetirməyə borcludurlar. Arbitraj qərarlarının yerinə yetirilməsi daha asandır, nəinki xarici məhkəmə qərarlarının.

Bu üsuldan mövcud beynəlxalq xüsusi hüququn İnternetlə bağlı həll edə bilmədiyi məsələlərlə əlaqədar yaranan boşluğu doldurmaq üçün geniş istifadə edilir. Arbitrajdan bu cür istifadəyə misal olaraq Domen adları haqqında mübahisələrə baxılması üzrə Vahid Siyasəti (MBVS) göstərmək olar [3]. MBVS Ümumdünya Əqli Mülkiyyət Təşkilatı (ÜƏMT) tərəfindən işlənib hazırlanıb

və *ICANN* tərəfindən mübahisələrin həlli üzrə əsas prosedur kimi qəbul olunub. MBVS arbitrajdan istifadəni əvvəlcədən yuxarı səviyyəli əsas ("köklü") domenlərin *(.com, .edu, .org, .net)* qeydiyyatı ilə bağlı bütün müqavilələrdə mübahisələrin həlli mexanizmi kimi şərtləndirilir. Arbitrajın unikallığı ondan ibarətdir ki, onun qərarları milli məhkəmələrin iştirakı olmadan bilavasitə domen adları sisteminə dəyişikliklərin edilməsi yolu ilə tətbiq edilir.

Ümumiyyətlə, qeyd etmək olar ki, arbitraj mübahisələrin daha sürətli, asan və ucuz başa gələn həlli yoludur. Amma arbitrajdan İnternetdəki mübahisələrin əsas həlli mexanizmi kimi istifadə edilməsində bir sıra mühüm çatışmazlıqlar var.

Birincisi, adətən, arbitraja müraciət edən tərəflər arasında ilkin razılaşma ilə şərtləndirildiyinə görə, bu üsuldan bir sıra hallarda istifadə etmək mümkün olmur. Məsələn, böhtan, kibercinayətkarlıq, müxtəlif növ cavabdehlik halları ilə bağlı tərəflər arasında əvvəlcədən razılıq əldə edilə bilməz.

İkincisi, bir çoxları bu praktikanı daha zəif tərəf üçün (adətən, elektron kommersiyadan istifadə edən alıcılar üçün) əlverişsiz hesab edirlər.

Üçüncüsü, bir çoxları narahatdırlar ki, arbitraj presedent hüququnu qlobal səviyyəyə qaldırır, bu da tədricən milli hüquq sistemlərinə təzyiq edilməsinə gətirib çıxaracaq. Kommersiya hüququna münasibətdə bu tendensiya az və ya çox dərəcədə qəbuledilməndir. Lakin İnternet materiallarının məzmunu sahəsində və sosial-mədəni aspektlərə münasibətdə milli hüquq normaları vacibdir, çünki öz ölkəsinin mədəni xüsusiyyətlərini əks etdirir.

Dördüncüsü, İnternetlə bağlı mövcud qanunvericilik göstərir ki, arbitraj məhkəmələri, o cümlədən MBVS əsasında fəaliyyət göstərənlər işgüzar sektorun maraqlarına qarşı daha loyaldırlar, nəinki vətəndaşların maraqlarına qarşı. Məsələn, Fransa məhkəməsi bu ölkənin "Danon" şirkətinin əleyhinə və *jeboycottedanone.com* (saytın adı "mən "*Danon*" şirkətini boykot edirəm" mənasını verir) saytını qeydiyyatdan keçirmiş onun narazı əməkdaşının xeyrinə qərar çıxartmışdı. Eyni zamanda, ÜƏMT-in MBVS-ə əsaslanan arbitrajı *Vivendi Universal* şirkətinin *vivendiuniversalsucks.com.* saytmın ləğv edilməsi barədə tələbini qəbul etdi. Hər iki halda domen adından etiraz və tənqid forması kimi istifadə edilirdi. Fransanın məhkəməsinin bu etiraz növünü qəbul etdiyi halda, ÜƏMT-in arbitrajının bunu qəbul etməyə hazır olmadığı üzə çıxdı [1].

5. ŞƏXSİ HƏYAT SİRRİNİN VƏ FƏRDİ MƏLUMATLARIN QORUNMASI PROBLEMLƏRİ

Şəxsi həyat sirrinin və fərdi məlumatların qorunması – İnternetin tənzimlənməsinin bir-biri ilə sıx bağlı olan aspektləridir. İnformasiyanın qorunması şəxsi həyatın qorunmasım təmin edən hüquqi mexanizmdir.

"Şəxsi həyat" anlayışımn tərifi konkret insan nöqteyi-nəzərindən asılıdır. Bəzi insanlar özləri haqqında məxfi informasiyamn bir hissəsinin açıqlanmasına etiraz etmir. Digər bir qisim isə şəxsi həyat sirlərini tamamilə qorumağa çalışır. "Şəxsi həyat" anlayışı həmçinin mədəni fərqlərdən asılıdır. Elə cəmiyyətlər var ki, onlar üçün məxfiliyin qorunması həyati əhəmiyyət kəsb edir, amma digər mədəniyyətlərdə bu məsələ o qədər də aktual olmaya bilər.

Göstərilən bu ziddiyyətlərə görə, "şəxsi həyat" terminino daha dəqiq tərif vermək zərurəti ortaya çıxır. Bu anlayışın müasir tərifi kommunikasiya sirrinə (yazışmaya nəzarətin edilməməsi) və özəl informasiyanın qorunmasına (özəl şəxslərə aid olan informasiyanı açıqlamamaq) istinad edir. Şəxsi həyat sirlərinin qorunması problemi ənənəvi olaraq, əsasən, fiziki şəxslərlə dövlət arasındakı münasibətlərə aid edilirdi. Lakin artıq problemin əhatə dairəsi olduqca genişlənib və buraya özəl sektor da daxil edilib.

"Fərdi məlumatlar – konkret insan haqqında, onunla eyniləşdirilən və ya eyniləşdirilə bilən (maddi daşıyıcıda əks olunmuş) informasiyadır. Fərdi məlumatlara bioqrafik və fərqləndirici (tanıdıcı) məlumatlar, şəxsi xarakteristika (xasiyyətnamə), ailə və sosial vəziyyət, təhsil, peşə, xidmət

və maliyyə vəziyyəti, sağlamlıq və s. vəziyyəti barədə məlumatlar aid edilir". Bu tərif Avropa Şurasının və Avropa Parlamentinin 24 oktyabr 1995-ci il tarixli "Fərdi məlumatların işlənib hazırlanması və bu məlumatlardan sərbəst istifadə ilə əlaqədar fiziki şəxslərin hüquqlarının qorunması haqqında" Direktivində öz əksini tapıb [6].

İP ünvanı – qurulmuş proqram təminatı və kompyuterin iş rejimi haqqında məlumatı, ilk növbədə, istifadə edilən informasiya texnologiyalarını identifikasiya edir. Əlavə informasiya olmadan həmin məlumatların istifadəçini identifikasiya etməsi barədə nəticə çıxarmaq mümkün deyil.

Ona görə də həmin informasiyanı fərdi məlumatlara aid etmək mümkün və ən əsası, vacib deyil. Yeri gəlmişkən, əgər belə edilərsə, onda bu ciddi dəyişikliklərə gətirib çıxara bilər. Bu zaman İnternetdəki informasiya mübadiləsi standartlarının və protokollarının çoxuna yenidən baxmaq lazım gələcək.

Birmənalı şəkildə qeyd etmək olar ki, elektron poçtu və istifadəçilər tərəfindən sərbəst şəkildə daxil edilən və onları identifikasiya etməyə imkan verən informasiyanı fərdi məlumatlara aid etmək lazımdır.

Ümumiyyətlə, informasiyanin toplanması informasiya resurslarının – veb-saytların məzmunu ilə tanış olarkən; loq-faylların məzmununu işləyərkən; elektron poçtdan istifadə edərkən (elektron məktubların başlıqları üzrə); provayderin modeminə qoşularkən və s. hallarda həyata keçirilə bilər.

Aşağıdakılar istifadəçi və onun kompyuteri haqqında informasiya əldə etmək üçün təşkilati-texniki imkana malikdirlər:

- istifadəçilərin daxil olduqları resursların sahibləri;
- elektron məktubları qəbul edənlər;
- istifadəçiyə xidmət göstərən provayder;
- ən müxtəlif məkrli niyyətləri olan üçüncü şəxslər;
- və s.

İstifadəçi haqqında informasiyanın əldə edilməsi aktiv və passiv ola bilər. Yəni müxtəlif xidmətlərdən istifadə hüququ əldə etmək üçün müəyyən elektron formaların doldurulması, habelə veb-resursda müxtəlif informasiyadan istifadə etmək üçün uyğun bölmələrin seçilməsi istifadəçinin aktiv fəaliyyətinin nəticəsidir. Həmçinin istifadəçinin İnternetə qoşulmasının, proqram təminatından və informasiya resurslarından, sistemlərindən istifadəsinin monitorinqini aparmaqla onun haqqında passiv məlumat alamaq olar.

Bu məlumatlar istifadəçini birmənalı olaraq identifikasiya edə bilər (məsələn, onun adı, soyadı, doğum tarixi, yaşadığı yer, peşəsi, iş yeri haqqında informasiyalar vasitəsi ilə). Həmçinin bu məlumatlar istifadəçinin İnternetə qoşulmaq üçün istifadə etdiyi aparat-proqram təminatının və informasiya sistemlərinin identifikasiyası üçün faydalı ola bilər.

İstifadəçinin kompyuteri vasitəsilə İnternetə qoşulmaq üçün edilən bütün hərəkətlər əksər hallarda dörd rəqəm blokundan ibarət olan və istifadəçinin qlobal şəbəkəyə qoşulmasını birmənalı olaraq identifikasiya edən İP ünvanları ilə fərdiləşdirilir. Həmin ünvan üzrə ümumi istifadədə olan serverlər vasitəsilə istifadəçinin provayderi haqqında mühüm informasiya əldə etmək olar.

Həmçinin İnternetdə işləyən şəxsin istifadə etdiyi proqram təminatı və kompyuterinin iş rejimi haqqında məlumat toplamaq mümkündür.

Yuxarıda göstərilənlərə əsaslanaraq belə nəticəyə gəlmək olar ki, istifadəçi İnternetdə işləyərkən onun haqqında əldə edilən məlumatlar geniş imkanlara malikdir. O cümlədən informasiya resurslarının keyfiyyətinin artırılması və İnternetdə biznes qurmaq üçün həmin məlumatlardan istifadə edilə bilər. Bu məlumatların köməyi ilə resurs istifadəçiləri üçün rahat iş şəraiti yaratmaq, həmçinin auditoriyanın tərkibini və üstünlüklərini analiz etmək olar.

Göstərilənlər, sözsüz ki, istifadəçi haqqında məlumatların yayılmasına xidmət edir. Amma brouzerlərin işləmə texnologiyası, proqram təminatının və əməliyyat sistemlərinin informasiya təhlükəsizliyi sahəsindəki çoxsaylı qüsurlar, istifadəçilərin müdafiəsiz olması, kompyuterlərinin imkanları və çatışmazlıqları barədə onlara məlumat verilməməsi, provayder heyətinin səhlənkarlığı, habelə bədniyyətli şəxslərin əməlləri İnternetdən informasiya əldə edən insanların informasiya hüquqlarının pozulmasma gətirib çıxarır.

Vətəndaşların informasiya hüquqlarının təmin edilməsi ilə bağlı olan bu problem, informasiya texnologiyaları və İnternetlə əlaqədar olan digər məsələlər kimi, onun həllinə texniki və təşkilati-hüquqi yanaşma tələb edir.

Texniki yanaşma istifadəçilərin və provayderlərin kompyuter sistemlərinin informasiya təhlükəsizliyi üçün çoxsaylı aparat-proqram təminatının yaradılmasını və yayılmasını, həmçinin xüsusi İnternet-servislərin yaradılmasını nəzərdə tutur.

Müxtəlif beynəlxalq hüquq normalarını ümumiləşdirsək, belə nəticəyə gəlmək olar ki, informasiya resursları və servisləri sahibləri, provayderlər, proqram təminatı istehsalçıları istifadəçilərlə işləyərkən aşağıdakı şərtlərə əməl etməlidirlər [24]:

- vətəndaşların şəxsi həyatma aid olan fərdi məlumatlarm toplanması və işlənməsi barədə onlara məlumat vermək;
- toplanan məlumatlarm növlərini və onların toplanma üsulunu açıqlamaq;
- toplanan məlumatlarm resurs, yaxud servis sahibləri və üçüncü şəxslər tərəfindən istifadə məqsədini və formasını göstərmək;
- istifadəçinin onun haqqında məlumatların toplanması və istifadəsinə münasibətinin xarakter və formasını ətraflı təsvir etmək;
- toplanmış məlumatların müddətini və formasını müəyyən etmək;
- istifadəçinin iradəsinə uyğun olaraq onun şəxsi həyatına dair informasiyanın olduğu məlumatların toplanmasını dayandırmaq imkanını reallaşdırmaq;
- vətəndaşın özü haqqında toplanan informasiya ilə tanış olmasına və dəqiqləşdirməsinə ödənişsiz imkan yaratmaq;
- istifadəçilərlə müvafiq münasibətlərin hansı qanunvericilik aktları ilə tənzimləndiyini müəyyən etmək;
- toplanan məlumatlarm qorunması rejimini pozmağa görə mülki məsuliyyətin hüdudlarını müəyyən etmək;

- istifadəçini vətəndaş haqqında məlumatların toplanması və onlardan istifadə ilə bağlı (o cümlədən operativ axtarış fəaliyyəti zamanı) qanunvericilikdə nəzərdə tutulan müddəalar barədə bilgiləndirmək.

Bir sıra xarici ölkələrdə İnternetdə istifadəçi haqqında məlumatları toplayarkən şəxsiyyətin maraqlarının təmin olunması probleminin təşkilati-hüquqi həlli aşağıdakılara əsaslanır [25]:

- şəxsiyyətin informasiya hüquqlarının müdafiəsini təmin edən ümumi normalar və bütövlükdə, fərdi məlumatların tənzimlənməsi institutu;
- informasiya texnologiyalarından istifadə edərkən müxtəlif növ məlumatların toplanmasına dair xüsusi maddi (predmet, əşya) normalar;
- özünütənzimləmə.

Qeyd etmək lazımdır ki, informasiya ərazi və əhali üzərində nəzarəti həyata keçirmək üçün hakimiyyət orqanları üçün həmişə olduqca vacib amil olub. İnformasiya texnologiyaları isə dövlətin informasiyanı toplamaq və analiz etmək sahəsindəki imkanlarını əhəmiyyətli şəkildə genişləndirir. Bu, həm hakimiyyət strukturları tərəfindən bilavasitə toplanan və emal edilən (vergi, əhalinin sosial müdafiəsi, səhiyyə, özəl mülkiyyət, məhkəmə işləri və s.), həm də əhaliyə əsas xidmətlər göstərən şirkətlərdə olan (elektrik, su sərfiyyatı, telekommunikasiya xidmətləri və s.) informasiyalara aiddir.

Verilənlərin işlənməsinə dair qabaqcıl texnologiyalar ayrı-ayrı sistemlərdən məlumatların toplanması və

inteqrasiyası, həmçinin məlumat massivlərindən qanunauyğunluqların, uyğunsuzluqların, qeyri-adi situasiyaların axtarılması üçün istifadə edilir.

Terrorçuluq, casusluq və dövlət əleyhinə yönələn digər fəaliyyət növləri şübhəli şəxslərin diqqətlə izlənməsini zəruri edir. İnsan hüquqlarının müdafiəçiləri isə milli təhlükəsizlik sahəsində daha sərt tədbirlərin həyata keçirilməsi ilə şəxsi həyat anlayışının tədricən öz mahiyyətini itirməsi barədə xəbərdarlıq edirlər.

Məsələn, bir neçə il bundan əvvəl kompyuterlərin *Clipper chip* adlanan unikal identifikasiya qurğusu ilə təmin edilməsi barədə təklif ictimaiyyət tərəfindən kəskin etiraz dalğasının yaradılmasına səbəb oldu [5]. Belə ki, müvafiq qurğu hakimiyyət orqanlarının istifadəçiləri izləməsi üçün "baca" rolunu oynaya bilərdi. Həmin vaxt insan hüquqlarının müdafiəçiləri qələbə çaldılar. Lakin son vaxtlar tarazlıq milli təhlükəsizliyin gücləndirilməsi hesabına yenidən pozulmaqdadır.

ABŞ-da federal səviyyədə bir sıra müvafiq qanunlar mövcuddur. Ən başlıcası isə, vətəndaşların informasiya hüquqlarının və İnternetdə istehlakçı hüquqlarının müdafiəsi sahəsində *Federal Trade Commission* (Federal Ticarət Komissiyası) adlı qurum olduqca fəaldır [1]. Bu təşkilat müvafiq sahədə geniş səlahiyyətə malikdir - tövsiyə xarakterli sənədlərin işlənib hazırlanmasından və elmi tədqiqatların aparılmasından başlamış İnternet xidmətləri ilə bağlı bütün şikayətlərin yoxlanması və müvafiq inzibati proseslərin yerinə yetirilməsinədək.

ABŞ-da uşaqların informasiya hüquqlarının müdafiəsi probleminə də xüsusi diqqət yetirilir. 1998-ci ildə bu problemin həllinə xidmət edən *Children's Online Privacy Protection Act* ("On-layn mühitdə uşaqların şəxsi

həyatının müdafiəsi" Aktı) qəbul edilib. Həmin qanun İnternetdə 13 yaşına qədər olan yetkinlik yaşına çatmayanların hüquqlarını veb-sayt və on-layn xidmət sahibləri tərəfindən onlar barəsində informasiyaların toplanması və istifadəsini qadağan etmək yolu ilə qoruyur [26].

2001-ci ilin 11 sentyabr hadisələrindən sonra ABŞ-da qəbul edilən "Vətənpərvərlik" Aktı (*Patriot Act*) və digər ölkələrin qəbul etdiyi analoji qanunlar elektron kommersiya üzərində daha ciddi nəzarətin həyata keçirilməsinə, o cümlədən məlumatların qanuni şəkildə ələ keçirilməsinə xidmət edirdi. Dəlil-sübutun toplanması məqsədilə informasiyanın qanuni yolla ələ keçirilməsi konsepsiyası Kibercinayətkarlıq üzrə Avropa Konvensiyasına da daxil edilib (20 və 21-ci maddələr) [6].

Şəxsi həyatı və məxfi məlumatların qorunmasını tənzimləyən əsas beynəlxalq sənəd 1980-ci ildə ATƏT tərəfindən hazırlanan Şəxsi həyatın və transmilli şəxsi məlumat axınının qorunması Prinsipləridir [27]. Bu prinsiplər və ATƏT-in sonrakı səyləri həmin sahədə bir sıra beynəlxalq və regional normaların yaradılmasına gətirib çıxartdı.

ABŞ-da bu problemin həlli özünütənzimləməyə əsaslanır [1]. Anonim iştirak hüququ ABŞ qanunvericiliyi ilə müdafiə olunur. Bu ölkədə dövlətin söz azadlığını məhdudlaşdırmağa yönələn istənilən cəhd Konstitusiya ilə ziddiyyət təşkil etdiyinə görə qanunsuz elan edilə bilər. Birləşmiş Ştatlarda inəxfiliyn təmin edilməsi siyasəti şirkətlər tərəfindən müəyyən edilir. Şirkətlər və fiziki şəxslərin özləri bu siyasətin hüdudlarını müəyyən edirlər.

Avropada fərdi məlumatların qorunması ilə bağlı münasibətlər aşağıdakı bir neçə normativ akt çərçivəsində tənzimlənir [6]:

- "Fərdi məlumatların avtomatlaşdırılmış işlənməsi ilə bağlı şəxsiyyətin müdafiəsi haqqında" Avropa Şurasının, 28 yanvar 1981-ci il tarixli, 108 saylı Konvensiyası. Bu sənəd fərdi məlumatı, şəxsi (məlumat subyektini) identifikasiya edən istənilən informasiya kimi müəyyən edir. Avtomatik işlənmə dedikdə isə, məlumatlarm toplanması, bu məlumatlarla məntiqi və ya riyazi əməliyyatların aparılması, onların dəyişdirilməsi, silinməsi, bərpası, yaxud yayılmasının tamamilə və ya qismən avtomatlaşdırılmış vasitələrin tətbiqi ilə həyata keçirilməsi nəzərdə tutulur.
- Avropa Birliyinin və Avropa Parlamentinin "Fərdi məlumatların işlənməsi və bu məlumatlardan sərbəst istifadə ilə əlaqədar fiziki şəxslərin hüquqlarının qorunması haqqında" 24 oktyabr 1995-ci il tarixli 95/46/ saylı Direktivi.
- Avropa Şurasının və Avropa Parlamentinin "Fiziki və hüquqi şəxs olan abonentlərin fərdi məlumatlarının işlənməsi və maraqlarının məxfiliyinin qorunması haqqında" 15 dekabr 1997-ci il tarixli 97/66/ saylı Direktivi. Bu sənəd informasiya subyektindən onun haqqında məlumatların toplanması, işlənməsi və yayılması ilə bağlı icazə alınmasına dair tələbləri müəyyən edir.

Göründüyü kimi, bu iki yanaşma (Amerika və Avropa) arasında ziddiyyət mövcuddur. Əsas problem

şəxsi məlumatların kommersiya strukturları tərəfindən istifadə edilməsi ilə bağlıdır. Məsələn, bu vəziyyətdə Avropa Birliyi ABŞ ərazisində yerləşən proqram təminatı üzrə şirkətin onun normalarına riayət etməsini təmin edə bilmir.

Bu əsaslı fərqlər müvafiq sahədə hər hansı bir razılaşmanın əldə edilməsini çətinləşdirir. Amerika qanunlarının Avropa qanunlarına uyğunlaşdırılması isə mümkün görünmür. Çünki bu proses Amerika hüquq sisteminin bəzi fundamental prinsiplərinin dəyişdirilməsini tələb edir. Vəziyyətdən çıxış yolu kimi ABŞ tərəfindən "təhlükəsiz liman" (*"safe harbor"*) təşəbbüsü irəli sürülüb [5]. Bu təşəbbüs diplomatik dalandan çıxmağa imkan verir.

Belə ki, həmin təşəbbüsə əsasən, Avropa Birliyi Amerika şirkətlərində "təhlükəsiz liman" prinsipini tətbiq etmək imkanına malikdir. Yəni Avropa Birliyi vətəndaşları haqqında informasiya ilə işləyən ABŞ şirkətləri məxfi informasiyanın qorunması ilə əlaqədar Avropa tələblərinə əməl etmək barədə könüllü olaraq öz üzərlərinə öhdəlik götürə bilərlər.

Virtual mühitdə şəxsi həyatın müdafiəsi ilə bağlı ABŞ və Avropa Birliyi arasındakı ziddiyyət göstərdi ki, elektron kommersiyanın yaratdığı qarşılıqlı asılılıq hər iki regionun ictimai və mədəni tarixində kök salmış müəyyən prinsipləri təhlükə altında qoyur. Qloballaşma digər ölkələrdə də oxşar situasiyaların yaranmasına gətirib çıxarır. "Təhlükəsiz liman" haqqında razılaşma Avropa Birliyi ilə digər ölkələr arasında da (Kanada və Avstraliya daxil olmaqla) analoji münasibətlərin qurulması üçün dəyərli presedent və faydalı vasitə kimi çıxış edir.

Dünyanın bir sıra ölkələrində İnternetdən istifadə zamanı vətəndaşların şəxsiyyətinin açıqlanması tələb

olunur [28]. Məsələn, Keniyada İnternet-provayderlərdən tələb edilir ki, öz abonentlərinin siyahısını təqdim etsinlər. Birmada isə İnternet-kafenin xidmətindən istifadə edənlər bunun üçün qeydiyyatdan keçməli və öz pasport məlumatlarını, ünvanlarını göstərməlidirlər. İtaliyada İnternet-kafeyə daxil olan hər bir istifadəçi öz pasportunu təqdim etməlidir. Hindistan polisi Maxaraştra ştatının hakimiyyət orqanlarından tələb edir ki, İnternet-kafelərə yalnız müvafiq filtrasiya proqramı qurulduqdan sonra lisenziya verilsin. Bundan başqa, istifadəçilər İnternetdən istifadə etmək üçün uzun bir anket doldurmalıdırlar.

Həmçinin dünyanın bir çox ölkələrində məhkəmələr İnternetdə elan verən, elektron poçt göndərişləri edən sıravi istifadəçilərin şəxsiyyətinin açıqlanması barədə qərar qəbul ediblər. Həmin istifadəçilər haqqında informasiya təqdim edilməsini nəzərdə tutan müəllif hüquqları şəxsi həyatın toxunulmazlığının qorunması sahəsində situasiyanı ağırlaşdırır.

Şəxsi həyatın toxunulmazlığı baxımından trafik haqqında məlumatların açıqlanması da problem yaradır. Bir sıra ölkələr trafik haqqında məlumatların terrorçuluqla mübarizədə son dərəcə vacib olduğunu dərk edərək həmin məlumatların saxlanmasına dair siyasət həyata keçirirlər [5]. 2001-ci ilin dekabrında Böyük Britaniyada qəbul olunan antiterror qanununda müvafiq məlumatların qorunması məsələsi də öz əksini tapıb. Fransa və digər Avropa Birliyi ölkələri də bu yolla getdilər. Həmçinin Cənubi Afrika və Argentina kimi ölkələr də bu təcrübədən istifadə etdilər. ABŞ-da hələlik müvafiq qanun qəbul edilməyib.

Yeni siyasət kütləvi nəzarətin həyata keçirilməsini və əldə edilən fərdi informasiyanın müxtəlif ölkələr tərəfindən

birgə istifadəsini nəzərdə tutur. Məsələn, mobil telefonlardakı məlumatlar cinayət işlərinin təhqiqatı ilə məşğul olan ABŞ və Fransanın hakimiyyət orqanları tərəfindən mübadilə edilə bilər.

Beləliklə, qeyd etmək olar ki, ayrı-ayrı ölkələr söz azadlığını və şəxsi həyatın toxunulmazlığını istədikləri kimi şərh edir, onları müxtəlif məqsədlərlə tənzimləyirlər, bunun üçünsə müxtəlif üsullardan istifadə edirlər. Demək olmaz ki, dövlətlərin fəaliyyəti söz azadlığını məhv etməyə yönəlib. Lakin onu da iddia etmək olmaz ki, İnternet söz azadlığının əsas mənbəyi və xilaskarıdır.

6. DOMEN ADLARI SİSTEMİNİN İDARƏ EDİLMƏSİ PROBLEMLƏRİ

İnternetə qoşulan hər bir kompyuter unikal İP ünvanına malikdir. Məhz İP ünvanı üzrə şəbəkədə qurğuların axtarışı və qarşılıqlı əlaqəsi həyata keçirilir. İP ünvanı bir-birindən nöqtələrlə ayrılan dörd rəqəm blokundan ibarət ardıcıllığı əks etdirir. Onu bu şəkildə yadda saxlamaq çox çətindir. Yadda saxlamanın və qavramanın rahat olması üçün İP ünvanma uyğun simvollardan ibarət domen adları sistemi (*Domain Name System - DNS*) yaradılıb. Məsələn, 62.212.230.18 əvəzinə - *www.science.az* yazmaq olar.

Beləliklə, müəyyən sayta daxil olmaq üçün kompyuter əvvəlcə *DNS*-serverə müraciət etməlidir. Həmin *DNS*-server sonra konkret saytın rəqəmsal ünvanını tapır. *DNS* dünyanın müxtəlif hissələrində yerləşən "əsaslı" serverlərdən, yuxarı səviyyəli domen serverlərindən və *DNS*-serverlər toplusundan ibarətdir [29].

Domen adları sisteminin idarə edilməsi İnternetin tənzimlənməsi məsələlərinin müzakirəsi zamanı həmişə qızğın mübahisələrin predmeti olub. Ən ziddiyyətli məqamlardan biri *DNS*-in iyerarxik quruluşu və son nəticədə ABŞ hökumətinin ona nəzarət etmək imkanıdır (Ticarət Nazirliyi vasitəsi ilə).

Domen adları ilə əlaqədar ictimai münasibətlərin təhlili üçün qeyd etmək lazımdır ki, mövcud domen adları sisteminin bir sıra xüsusiyyətləri vardır [14]:

- *DNS* bütün İnternet şəbəkəsi üçün vahid sistemdir və iyerarxik quruluşa malikdir;

- *DNS* könüllü bir sistemdir və insanlara sərbəst olan domen adlarını seçmək və qeydiyyatdan keçirmək imkanı verir;
- qeydiyyatdan keçirilmiş domenlər üçün onların İnternetin bütün ünvan məkanında unikallığı təmin edilir;
- iqtisadi sistem ödənişli əsaslara söykənir.

Yuxarıda göstərilən xüsusiyyətlərə əsaslanaraq qeyd etmək olar ki, domen adları – mahiyyətinə görə fərdiləşdirmə vasitəsidir. Belə ki, istehlakçılara və istifadəçilərə virtual məkandan səmərəli istifadə etməyə imkan verir.

Göstərilən ictimai münasibətlərdə domenin gələcək sahibi və qeydiyyatçı – bu və ya digər birinci səviyyəli domen zonasının domen adlarının verilənlər bazasına yazını daxil etmək hüququ olan səlahiyyətli təşkilatdır. Qeydiyyat prosesində həmçinin vasitəçilərin – İnternetdə xidmətlərin göstərilməsi üzrə ixtisaslaşan şəxslərin iştirakı mümkündür. Bunlardan başqa, həmin münasibətlərdə domen adlarından istifadə ilə bilavasitə əlaqədar olaraq provayderlər – domen sahibinin informasiya resursuna texniki dəstək üzrə xidmət göstərən təşkilat da iştirak edir.

Göstərilən subyektlər arasında qeydiyyatçı mühüm rol oynayır [1]. Bu subyekt domen adını seçmir, amma özünün xüsusi statusu hesabına bir inhisarçı kimi bütün qeydiyyat və domen adlarmdan istifadə prosesləri üzərində təşkilati-texniki nəzarəti həyata keçirmək imkanına malikdir. Yalnız qeydiyyatçıdan asılıdır ki, domen adı və onun sahibi haqqında hansı informasiya *DNS*-server üzrə yayılacaq; nə vaxt bu və ya digər adın sahibi dəyişəcək; nə vaxt qeydiyyat ləğv ediləcək və ünvan hamı üçün əlyetərli

olacaq, adın özünü isə yenidən qeydiyyatdan keçirmək mümkün olacaq.

Bu münasibətlərdə daha bir xüsusi məqam ondan ibarətdir ki, qeydiyyata alınmış domenlər yüksək dövriyyə qabiliyyətinə malikdir. Belə ki, domen sahiblərinin dəyişməsi (yenidən qeydiyyatı) prosesi olduqca qısa müddətdə yerinə yetirilir. Bu xüsusiyyət İnternetin olduqca operativ mühit olduğunu bir daha təsdiq etsə də, sabit hüquqi mexanizmlərin köməyi ilə, o cümlədən məhkəmə vasitəsilə öz maraqlarını qorumağa çalışan resurs sahiblərinə əlavə problemlər yaradır.

Domen adlarını qeydiyyatdan keçirdikdən sonra ondan müxtəlif məqsədlər üçün istifadə edilə bilər [1]:

- domen adının sahibi həm fiziki, həm də hüquqi şəxs ola bilər;
- qeydiyyatdan keçirilən domen adları aktiv də ola bilər, passiv də (hər hansı informasiya resursuna müraciət üçün istifadə edilə də bilər, edilməyə də);
- elektron poçt xidməti üçün istifadə edilir;
- açıq və hamı üçün əlyetərli informasiya resursunun ünvanı kimi çıxış edir;
- hər hansı bir informasiya olmayan səhifəyə müraciət üçün istifadə edilir;
- məhdudlaşdırılmış giriş imkanı olan (istifadəçinin qeydiyyatdan keçməsi tələb edilən) informasiya resursunun ünvanı kimi istifadə edilir;
- informasiya resursunun digər ünvanına göndərmək üçün təşkil edilir;

- reklam xarakterli informasiyaya malik ola bilər, sahibinin kommersiya fəaliyyətinə dəstək vermək üçün istifadə edilə bilər;

Domen sahiblərinin bu adları qeydiyyatdan keçirərkən və onlardan istifadə edərkən mülki dövriyyə iştirakçılarının hüquqlarının pozulması hallarına da tez-tez rast gəlinir.

Domen adlarının qeydiyyatı və onlardan istifadə ilə bağlı mübahisələrə dair mövcud məhkəmə praktikasına baxdıqda görmək olur ki, daha çox mülkiyyət hüququnun obyektləri – firma adları və əmtəə nişanları ilə bağlı qanun pozuntularına yol verilir.

Bundan başqa, domen adlarının qeydiyyatı və istifadəsi zamanı həmçinin fiziki şəxslərin, coğrafi obyektlərin, kütləvi informasiya vasitələrinin, idman komandasının, yaxud məşhur bədii əsərlərin adları ilə bağlı da hüquq pozuntuları müşahidə olunur.

Domenlərin idarə edilməsinin mühüm hissəsi ticarət markalarının qorunması və mübahisələrin həll olunmasıdır. İnternetin ilk dövrlərində domen adlarının qeydiyyatı "birinci kim gəlsə, ona xidmət edilir" prinsipinə əsaslanırdı, yəni istənilən şəxs istədiyi adı qeydiyyatdan keçirə bilərdi. Domen adlarının potensial dəyəri kiberskvottinq (domen adlarının sonradan satmaq məqsədi ilə qeydiyyatı - möhtəkirlik) adlanan fəaliyyəti meydana gətirdi. İki domenin eyni adla fəaliyyət göstərməsinin qeyri-mümkünlüyü qeydiyyat hüququ ilə bağlı mübahisələrə yol açdı. Bu problem tanınmış markalardan (məsələn, *Microsoft, Nike, Toyota, Rolex*) istifadə edən domen adları üçün xüsusi əhəmiyyət kəsb etməyə başladı [5].

1999-cu ildə *ICANN* tərəfindən İnternet üçün mühüm əhəmiyyət kəsb edən iki normativ sənəd – "Domen adları

ilə bağlı mübahisələrə baxılmasına dair vahid Siyasət" (*UDRP*) və "Domen adları ilə bağlı mübahisələrə baxılmasına dair vahid siyasət üçün Qaydalar" qəbul edildi [3]. Həmin sənədlər domen adlarının istifadəsi ilə bağlı beynəlxalq münasiflər məhkəməsinin tamamilə yeni prosedurunu müəyyən edir.

Bu Siyasət və Qaydalar vasitəsilə mübahisələrə prinsipcə yeni məhkəmədənkənar baxılma sistemi yaradıldı. Tribunallar əmtəə nişanının mülkiyyətçisi ilə oxşar domen adı sahibi arasındakı mübahisələri xüsusi arbitraj mərkəzləri çərçivəsində yaradılan bu sistemdən istifadə etməklə həll edirlər. Bu cür qərarların legitimliyi *.com*, *.net*, və *.org* zonalarında istənilən domen adının qeydiyyatına dair müqavilədə göstərilən standart qeyd-şərtə uyğun olaraq təmin edilir.

ICANN –ın müvafiq Siyasət və Qaydaları qüvvəyə mindikdən indiyə kimi domen mübahisələri ilə bağlı məsələləri həll etmək səlahiyyəti verilən bir sıra arbitraj mərkəzləri qeydiyyatdan keçib.

Domen adları haqqında mübahisələrə baxılmasına dair vahid Siyasət tərəfindən *DNS* sisteminin idarə edilməsi sahəsində aparılan islahatlar nəticəsində kiberskvottinq fəaliyyətini əhəmiyyətli dərəcədə məhdudlaşdıran mexanizmlər tətbiq edildi. *UDRP* -nin yalnız *.com, .net* və *.org* domenlərinə aidiyyəti var, ölkə kodlarına əsaslanan domenlərin fəaliyyətinə toxunmur.

Arbitraj mərkəzləri eyni zamanda üç əsas olarsa, domen adını cavabdehdən alıb iddiaçıya verir [1]:

1. domen adı iddiaçının əmtəə nişanı ilə identik (eyni) və ya qarışıq salma dərəcəsində oxşar olduqda;

2. cavabdehin mübahisəli domen adı ilə bağlı hüquqları və ya qanuni maraqları olmadıqda;
3. domen adı cavabdeh tərəfindən qeydiyyatdan keçirilmiş olduqda və bilavasitə istifadə edildikdə.

Domen adları ilə bağlı daha bir mübahisəli məqam onların hüquqi statusu ilə bağlıdır. Bu məsələ ilə bağlı iki yanaşma üstünlük təşkil edir.

İnternet-hüquq üzrə hüquqşünasların bir hissəsi hesab edir ki, domen adı – mülkiyyətdir, domen adına olan hüquq isə - mütləq mülkiyyət hüququdur.

Avropa İnsan Hüquqları Məhkəməsinin (AİHM) domen adları ilə bağlı hüquqların statusuna dair 18 sentyabr 2007-ci il tarixli qərarı da bu mövqeni dəstəkləyir [30]. Qərarda göstərilir ki, domen adının sahibi ondan istifadə üsullarını müstəqil şəkildə müəyyən etmək hüququna malikdir. Ona görə də domen adlarından istifadəyə dair müstəsna hüquq iqtisadi dəyərə malikdir, yəni eyni zamanda, mülkiyyət hüququ sayılır.

Digər hüquqşünasların fikrincə, domen adına olan hüquq müqavilə əsasında yaranır və ona görə də bu hüquq nisbi xarakter daşıyır, domen adı isə - sadəcə, bağlanmış müqavilə üzrə registrator xidmətidir [5].

DNS-in idarə edilməsinin mövcud strukturunun digər mühüm tərkib hissəsi yuxarı səviyyəli milli domenlərin idarə edilməsidir. Hazırda milli domenləri İnternetin inkişafının ilkin dövrlərində, dövlətlərin bu məsələlərlə ciddi maraqlanmadığı vaxtlarda lisenziya alan müxtəlif institutlar idarə edir. Onların arasında elmi müəssisələr, texniki assosiasiyalar, QHT-lər və hətta fiziki şəxslər də var. Bir çox hallarda ölkə kodları ilə idarəetmə hüququ da "birinci kim gəlsə, ona xidmət edilir" prinsipi üzrə verilir.

DNS-ə iki tip yuxarı səviyyəli domen daxildir [14]. Birinci tip – ümumi domenlər, ikinci tip – ölkə kodlarına əsaslanan domenlərdir. Yuxarı səviyyəli ümumi domenlərə bunlar aiddir:

- *.com, .edu, .gov, .mil* və *.org* (1984-cü ildən);
- *.net* və *.int* (1985-ci ildə əlavə edilib);
- *.biz, .info, .name, .pro, .museum, .aero* və *.coop* (2000-ci ildə əlavə edilib).

Hər bir yuxarı səviyyəli ümumi domen üçün ünvan siyahısını bir registratura dəstəkləyir. Məsələn, *.com* domeni *VeriSign* şirkəti tərəfindən idarə edilir. "Satıcı" funksiyasını registratorlar öz üzərlərinə götürürlər. *ICANN* müqavilə bağlayaraq və registraturalara, həmçinin registratorlara lisenziya verərək, *DNS* sisteminin ümumi koordinasiyasını həyata keçirir.

Bu təşkilat həmçinin topdansatış qiymətlərini təyin edir (həmin qiymətlər əsasında registratura domen adlarını registratorlara icarəyə verir), registraturanın və registratorların göstərdikləri xidmətlərə dair müəyyən şərtləri təsdiq edir. Beləliklə, *ICANN* yuxarı səviyyəli ümumi domen adları bazarında iqtisadi və hüquqi məsələlər üzrə tənzimləyici orqan qismində çıxış edir.

Milli domenlərin idarə edilməsi

Yuxarı səviyyəli milli domenlərin idarə edilməsi ilə bağlı üç vacib problem mövcuddur. Birincisi, tez-tez siyasi cəhətdən ziddiyyət doğuran qərarla bağlıdır. Belə ki, ölkənin, yaxud muxtar ərazinin beynəlxalq statusu qeyri-müəyyən və ya mübahisəli olduqda hansı milli kodların qeydiyyata alınmalı olması məsələsi problem doğurur. Problemdən çıxış yolu kimi, İnternetdə tətbiq edilən

şəbəkə protokollarının əsas müəlliflərindən biri olan C.Postel milli domen adlarının bütün ölkələrin və digər muxtar ərazilərin ikihərfli kombinasiyalarla adlandırıldığı *ISO* standartlarına uyğun olaraq paylanmasını təklif etdi. C.Postelin bu yanaşması uğurlu alındı və indiyə qədər tətbiq edilir [5].

İkinci məsələ milli kodların kim tərəfindən idarə edilməsi ilə bağlıdır. Bir çox ölkələr öz domenlərini milli sərvət hesab edərək, onlar üzərində nəzarəti ələ almağa cəhd göstərirlər. Məsələn, CAR öz suveren hüququndan milli domen üzərində nəzarətin özünə qaytarılması üçün arqument qismində istifadə etmişdi. Bu məqsədlə qəbul edilən qanuna uyğun olaraq milli domendən CAR hökuməti tərəfindən müəyyən edilənlərdən başqa hər hansı məqsəd üçün istifadə edilməsi cinayət sayılır. Çoxtərəfli yanaşmanın uğurlu nümunəsi kimi, adətən, milli domenlərin idarə edilməsinin Braziliya modeli göstərilir. Braziliya domenlərini idarə edən milli orqan hakimiyyət orqanları, biznes sektoru və vətəndaş cəmiyyəti də daxil olmaqla, bütün maraqlı tərəflər üçün açıqdır.

Əksinə, milli domenlərin idarə edilməsinin hökumətə verildiyi Kambocanın təcrübəsi səlahiyyətlərin verilməsinin uğursuz nümunəsi adlandırılır. Belə ki, hökumət xidmətlərin keyfiyyətini aşağı salıb və milli domenlərin qeydiyyatını çətinləşdirən yüksək rüsumlar tətbiq edir.

Üçüncü məsələ bir çox ölkələrin domen operatorlarının *ICANN* sisteminin bir hissəsinə çevrilmək istəmələri ilə bağlıdır. İndiyə kimi *ICANN* bütün milli domen operatorlarını öz "qanadı altına" ala bilməyib. Bəzi milli domen operatorları Avropa yuxarı səviyyəli

domenlərinin milli registratura Şurası kimi öz xüsusi regional təşkilatlarını yaradıblar [4].

Dil problemi: çoxdilli domen adları

İnternetdə dil müxtəlifliyi informasiya cəmiyyətinin müxtəlif aspektlərinin müzakirəsi zamanı əsas məsələlərdən biri kimi nəzərdən keçirilir. Qlobal şəbəkənin gələcək inkişafına mane olan əsas problemlərdən biri də İnternet-infrastrukturunun idarə edilməsində çoxdilli metodların çatışmamasıdır. İnternet yarananadan bəri domen adları yalnız ingilis dilində qeydiyyata alınır və istifadə edilirdi. Hətta *ASCII* standartına uyğun gəlməyən alman və fransız əlifbasının simvolları İnternet ünvanlarında istifadə edilə bilməzdi [5]. Daha mürəkkəb vəziyyət latın əlifbasının istifadə edilmədiyi yazı sistemi ilə bağlı idi.

Yuxarı səviyyəli çoxdilli domenlər sahəsindəki çoxsaylı proqram təminatı arasında ən aktual olanlar "beynəlmiləlləşdirilən domen adları" (*Internationalized Domain Names - IDN*) və "ana dilində İnternet ünvanları" (*Native Language Internet Address - NLIA*) sistemləridir [3]. İİİQ tərəfindən təklif edilən texniki proqram təminatı - *IDN* tədricən həlledici mövqe tutmağa başlayır. *IDN* birbaşa istifadəçinin kompyuterində digər dillərdə olan domen adlarını ingilis dilinə çevirir və sonra ingilisdilli domen adı əsasında *DNS*-sorğu göndərir. *IDN*-dən daha geniş istifadə edilməsinin qarşısındakı ən böyük maneələrdən biri onun *Internet Explorer* kimi əsas İnternet-brauzerlərə tam inteqrasiyasıdır.

Texniki çətinliklərdən başqa, daha bir (bəlkə də ən çətin) problem idarəetmə siyasətinin və prosedurunun hazırlanmasıdır. Əhalisi eyni dildə danışan ölkələrdə və ya

ölkə qruplarında idarəetmənin hissə-hissə *IDN* sisteminə ötürülməsi ideyası getdikcə daha fəal şəkildə yayılır. Belə ki, Çin hökuməti bir neçə dəfə bildirib ki, bu ölkənin dilində olan *IDN*-ni onun özü idarə etməlidir. *IDN* sisteminin idarə edilməsi siyasətinin işlənib hazırlanması və həyata keçirilməsi ən ciddi çağırışlardan biri olacaq.

2003-cü ildə YUNESKO-nun Baş Konfransı tərəfindən qəbul edilən "Kibermәkanın əlyetərliliyi üçün çoxdilliliyin inkişafı və istifadəsinə dair Tövsiyələr" müvafiq problemin həlli istiqamətində mühüm addım idi. Bu sənəddə dövlət və özəl sektora, milli, regional və beynəlxalq vətəndaş cəmiyyəti qurumlarına İnternetdəki dil maneələrini aşmaq, insanların interaktiv ünsiyyətini inkişaf etdirmək, əlyetərliliyi təmin etmək məqsədilə müvafiq tədbirlərin görülməsi tövsiyə edilir [31].

Həmin sənədə uyğun olaraq 2008-ci ildə *ICANN* tərəfindən İnternetdən istifadənin sərhədlərinin əhəmiyyətli dərəcədə genişlənməsinə imkan verən yeni konsepsiya qəbul edildi [3]. Bu konsepsiyada yuxarı səviyyəli domen adlarının əlifbası ilə yanaşı, bir sıra digər dillərdə də yazılmasının mümkünlüyü qeyd edilirdi.

ICANN-ın 2009-cu ilin oktyabr ayının 30-da Cənubi Koreyanın paytaxtı Seul şəhərində keçirilən sessiyasında isə artıq domen adlarının latın qrafikasına əsaslanmayan bir sıra əlifbalarda – rus, çin, ərəb, ivrit, hindu, koreya və s. əlifbalarda qeydiyyata alınması barədə qərar qəbul etdi. Artıq noyabr ayının 16-dan *ICANN* qeyri-latın əlifbasında olan domen adlarının qeydiyyatı ilə bağlı ərizələri qəbul etməyə başlayıb. Daha çox çin və ərəb dilində olan domen adlarının qeydiyyatı ilə bağlı ərizələrin daxil olacağı proqnozlaşdırılır.

7. İNTERNET-PROVAYDERLƏRİN MƏSULİYYƏTİNİN MÜƏYYƏN EDİLMƏSİ PROBLEMLƏRİ

İnternet-provayder (*Internet Service Provider, ISP*) – İnternetə daxil olma, burada informasiyanın yerləşdirilməsi, ötürülməsi və bu qlobal şəbəkə ilə bağlı digər xidmətlər göstərən təşkilatdır [32].

İnternet provayderləri müxtəlif cür adlandırılır: *ISP, ASP*, informasiya elanları xidmətinin sahibləri [1]. Avropa qanunvericiliyində *intermediary service providers* (vasitəçilik xidməti provayderləri), Amerika praktikasında isə *on_line service provider* (on-layn xidmət provayderləri), *provider of access* (qoşulma provayderləri), *provider of the informational content* (informasiya məhsulları provayderi) terminlərindən istifadə edilir. Rusiya qanunvericiliyində isə "informasiya vasitəçisi" termini işlədilir.

Qeyd etmək lazımdır ki, provayderlərin məsuliyyət problemi – dövlət siyasətinin təkcə İnternet sahəsində deyil, ümumiyyətlə, milli təhlükəsizlik sferasında çox mühüm problemlərindən biridir. Bir çox dövlətlərin nəzərincə, onlar İnternet üzərində nəzarətin yaradılmasının və istifadəçilərin hüquq normalarına riayət etmələrinin təmin edilməsinin ən sadə, aşkar mexanizmidir.

İnternet-provayderlərin göstərdikləri xidmətlərin müəyyən özəllikləri var. Provayder informasiya münasibətlərinin təşəbbüskarı kimi çıxış etmir, ötürülən informasiyanın məzmununu və istifadəçisini seçmir, informasiyanın məzmununa təsir göstərmir, informasiyanı texniki standartlarda və protokollarda müəyyən edildiyi

qaydaya uyğun olaraq yalnız müəyyən müddət üçün saxlayır.

1990-cı illərdə - İnternetin canlanması zamanı provayderlər istifadəçilər tərəfindən yerləşdirilən, yaxud baxılan materialların məzmununa və ya müəllif hüquqlarına görə heç bir məsuliyyət daşımırdılar [1]. Belə bir fikir yayılmışdı ki, provayderlərə əlavə təzyiqlərin edilməsi İnternetin gələcək inkişafına əngəl törədir. İnternetin kommersiya əhəmiyyətinin artması və təhlükəsizlik məsələlərinin aktuallaşması nəticəsində bir çox ölkələr provayderlərdən qanunlara riayət edilməsi aləti kimi istifadə etməyə başladılar.

Provayderlərin məsuliyyəti onların təşkilati-texniki imkanlarına əsaslanır. Onlar istənilən vaxt öz istifadəçilərinin ictimai informasiya münasibətlərinə təsir göstərə bilirlər. Təsir forması müxtəlif ola bilər: informasiya mübadiləsinə qadağa qoymaqdan başlayaraq üçüncü şəxsləri ötürülən informasiyanın məzmunu barədə məlumatlandırmağa qədər.

Beynəlxalq praktikada provayderlərin məsuliyyəti ilə bağlı 3 cür yanaşma var [1]:

1. Provayder istifadəçilərin heç də bütün fəaliyyətinə görə məsuliyyət daşımır. Baxmayaraq ki, istifadəçilərin hər bir fəaliyyəti barədə provayderdə məlumat olur.
2. Provayder istifadəçilərin fəaliyyətinə görə o halda məsuliyyət daşımır ki, informasiya mübadiləsi subyektləri ilə qarşılıqlı münasibətin və onlara göstərilən xidmətlərin xüsusiyyətləri ilə əlaqədar müəyyən şərtləri yerinə yetirir.

3. Provayder istifadəçilərin heç bir fəaliyyətinə görə məsuliyyət daşımır.

Müxtəlif ölkələrin qanunvericiliyi provayderlərin məsuliyyəti problemini yuxarıda göstərilən 3 sxemə uyğun olaraq həll edilməsini təklif edir [5]. Məsələn, əgər Çində və Yaxın Şərq ölkələrində 1-ci yanaşma tətbiq edilirsə, ABŞ-da 3-cü yanaşmaya (əksər hallarda provayderlər toxunulmazlıq hüququna malikdir və öz istifadəçilərinin fəaliyyətinə görə məsuliyyət daşımır), Avropada isə 2-ci yanaşmaya üstünlük verilir. Müvafiq məsuliyyət məsələsi ilə bağlı daha geniş hüquqi normalar Elekton Kommersiya üzrə Avropa Direktivində öz əksini tapıb. Direktivdə müəyyən edildiyinə görə, provayder ötürülən informasiya ilə əlaqədar o halda məsuliyyət daşımır ki, informasiyanın ötürülməsinə təşəbbüs göstərmir, informasiya istifadəçisini seçmir və ötürülən informasiyanın tamlığına təsir göstərmir.

İnternetdə ünsiyyət azadlığı haqqında Avropa Şurası Konvensiyasının prinsiplərindən biri məhz provayderlərin İnternet kontentlərinə nəzarət üzrə məsuliyyətinin məhdudlaşdırılmasını əks etdirir [6]. Sənəddə qeyd olunur ki, üzv dövlətlər provayderlərin üzərinə İnternet-resursların məzmununa nəzarət etmək vəzifəsi qoymamalıdırlar.

Telekommunikasiya inhisarçılığının mövcud olduğu ölkələrdə telekommunikasiya qurumlarının özləri İnternet xidməti göstərirlər [33]. İnhisarçılar provayderlərin bazara çıxışını əngəlləyirlər və rəqabətin inkişafına imkan vermirlər. Nəticədə yüksək qiymətlər müəyyən edilir, xidmətin keyfiyyəti aşağı səviyyədə qalır və rəqəmsal fərqlərin aradan qaldırılması mümkün olmur. Bəzi hallarda telekommunikasiya inhisarçıları digər İnternet-provayderlərin fəaliyyətinə dözürlər, amma onların işlərinə

bilavasitə qarışırlar (məsələn, buraxılış imkanlarının məhdudlaşdırırlar və ya xidmət göstərilməsinə maneçilik törədirlər).

Hüquq sistemlərinin çoxunda belə bir ümumi prinsip var ki, əgər provayder onun göstərdiyi xidmətdən müəllif hüquqlarını pozan materialların yerləşdirilməsi üçün istifadə edildiyini bilmirsə, buna görə məsuliyyət daşıya bilməz. Bu sistemlər arasında əsas fərq provayderin onun serverində yerləşdirilən materialın müəllif hüquqlarını pozduğu barədə məlumatlandırdığına baxmayaraq, onu silmədiyi halda, hansı hüquqi tədbirin görülməsi ilə bağlıdır.

ABŞ və Avropa Birliyinin qanunları "xəbərdarlıq etmək-silmək" prosedurunu nəzərdə tutur [5]. Buna uyğun olaraq provayder müvafiq materialı silməlidir ki, məhkəmə prosesinə cəlb olunmasın. ABŞ və Avropa Birliyinin qanunları materialdan istifadə edən şəxsin buna görə dəlil gətirməsinə imkan vermədən müəllif hüquqları daşıyıcılarının maraqlarını daha ciddi şəkildə qoruyur.

İnternet-provayderlər, istər-istəməz, tədricən informasiya materiallarının tənzimlənməsi üzrə siyasətə cəlb olunurlar [24]. Onların iki seçim imkanı var:

- Birincisi – hakimiyyət orqanları tərəfindən işlənib hazırlanan normalara riayət etmək.
- İkincisi – özünütənzimləməyə əsaslanaraq, hansı materialların yerləşdirilməsinin məqbul olduğunu müstəqil şəkildə müəyyənləşdirmək. Bu variant İnternet-resursların məzmununa münasibətdə siyasətin "özəlləşdirilməsi" riski ilə bağlıdır – bu zaman provayderlər hakimiyyət funksiyalarını öz üzərlərinə götürməlidirlər.

Bir çox ölkələrdə qəbul edilmiş qanunvericilik normaları provayderlərin üzərinə İnternet materiallarının tənzimlənməsi üzrə xüsusi vəzifələr qoyur [5]. Bu, həm onların serverlərində yerləşdirilən, həm də onların müştərilərinin çıxış əldə etdikləri materiallara aiddir.

İnternet-provayderlərin fəaliyyətinin telefon xidməti təşkilatı kimi tənzimlənməsi kontentə nəzarətlə bağlı məsuliyyətin bir hissəsini onların üzərindən götürür. Eyni zamanda, onları rabitə sahəsindəki çoxsaylı tənzimləyici normalara tabe etdirir. İnternetə televiziya və radio kimi geniş yayım mühiti kimi yanaşılması İnternet-provayderlərin üzərinə onların kanalları vasitəsilə yayılan kontentlərə görə məsuliyyət qoyur. Biznes modelindən asılı olaraq bəzən İnternet-provayderlər könüllü olaraq öz üzərlərinə belə məsuliyyət götürürlər, amma əksər hallarda müvafiq məsuliyyət qanunla müəyyən edilir.

Ayrı-ayrı dövlətlərdə bu məsuliyyət də fərqlidir. Bu da konkret bir dövlətdə İnternetin statusunun necə müəyyən edilməsindən asılıdır. Məsələn, Əlcəzair qanunvericiliyinə görə, bütün İnternet-provayderlər saytlarda yerləşdirilən kontentlərə görə məsuliyyət daşıyır. İsveçrə qanunvericiliyində isə İnternet-provayderlər yalnız müəllifini müəyyən etmək mümkün olmayan kontentlərə görə məsuliyyət daşıyır. Macarıstan qanunvericiliyinə görə, İnternet-provayderlər yalnız saytın qanunu pozduğu barədə məlumatlandırıldığı, lakin bununla əlaqədar heç bir tədbir görmədiyi halda məsuliyyət daşıyır.

Qeyd etmək lazımdır ki, İnternetə çıxış arxitekturu üç qatdan ibarətdir. Son istifadəçiləri İnternetə qoşan provayderlər üçüncü qatı təşkil edirlər. Birinci və ikinci qatlar genişzolaqlı rabitə xidmətlərinin topdansatış provayderlərindən ibarətdir [33]. Birinci qata (İnternet-

magistrallar), adətən, *MCI, AT&T, Cable Wireless və France Telecom* kimi iri şirkətlər tərəfindən nəzarət edilir. Ənənəvi telekommunikasiya şirkətləri qlobal bazarda İnternet-magistrallar sahəsində də dominatlıq edirlər. İkinci qatı təmsil edən provayderlər, adətən, milli və ya regional səviyyədə fəaliyyət göstərirlər.

İnternet məlumatları istənilən kommunikasiya kanalı vasitəsilə ötürülə bilər. Lakin praktikada birinci qat magistralı kimi kommunikasiya vasitələri İnternetin fəaliyyəti üçün xüsusi əhəmiyyət kəsb edir. Onların İnternetin strukturunda mühüm yer tutması sahiblərinə qiymətləri müəyyən etmək və göstərdikləri xidmətlərə görə öz şərtlərini diktə etmək imkanı verir.

İnternet-provayderlərin hansı dərəcədə Ümumdünya Ticarət Təşkilatının (ÜTT)-nin fəaliyyət qaydaları altına düşməli olub-olmadığı ilə bağlı ziddiyyətli baxışlar mövcuddur [34]. İnkişaf etmiş ölkələr göstərirlər ki, ÜTT tərəfindən telekommunikasiya operatorlarına təqdim edilən liberal qaydalar İnternet-provayderlər üçün də tətbiq edilə bilər. Məhdud traktovka tərəfdarları isə iddia edirlər ki, ÜTT rejimi yalnız telekommunikasiya bazarı üçün keçərlidir, İnternet-provayder bazarının tənzimlənməsi ÜTT çərçivəsində yeni qaydaların işlənib hazırlanmasını tələb edir.

Qeyd etmək lazımdır ki, provayderlərin məsuliyyəti ilə bağlı problemlər İnternetdən istifadəyə dair dövlət siyasətinin ən aktual məsələlərindən biridir. İnternetdəki ictimai informasiya münasibətlərində provayderlərin rolunun necə müəyyən edilməsindən və reqlamentləşdirilməsindən asılı olaraq, bu qlobal şəbəkənin inkişafında müxtəlif istiqamətlər yarana bilər.

İnkişaf etmiş və inkişaf etməkdə olan ölkələr arasındakı rabitə xərclərinin ödənilməsi problemləri

İnternet-provayder xidmətləri ilə bağlı daha bir mühüm problem İnkişaf etmiş və inkişaf etməkdə olan ölkələr arasındakı rabitə xərclərinin ödənilməsi ilə bağlıdır [33]. Hazırda bu xərclər, əsasən, inkişaf etməkdə olan ölkələrin hesabına örtülür. Ənənəvi telefon sistemində hər bir beynəlxalq danışıq xərcləri iki ölkə arasında bölünür. Lakin İnternetdə qəbul olunan model bütün yükü bir tərəfin – əsasən, inkişaf etmiş ölkələrdə yerləşən magistrallara qoşulan inkişaf etməkdə olan ölkənin üzərinə qoyur. Paradoksal olsa da, bu, bir faktdır ki, kiçik və yoxsul ölkələr inkişaf etmiş ölkələrdə İnternetə subsidiya ayırırlar.

Pul hesablaşmaları problemi daha yoxsul ölkələr üçün xüsusilə vacibdir. Həmin ölkələrdə beynəlxalq kommunikasiyalardan əldə edilən gəlir büdcənin doldurulması üçün mühüm mənbə kimi çıxış edir. İnternet-telefoniyanın (*VoIP*) yaranması və yayılması vəziyyəti daha da mürəkkəbləşdirdi. Bunun nəticəsində telefon danışıqlarının böyük bir hissəsi milli operatorlar deyil, İnternet vasitəsilə aparılmağa başlandı.

BTİ-nin təşəbbüsü ilə mövcud İnternet xərclərinin örtülməsi sisteminin mümkün təkmilləşdirilməsi ilə bağlı danışıqlara başlanmışdır. Məqsəd İnternetə çıxış xərclərinin daha tarazlaşdırılmış şəkildə bölüşdürülməsidir. Lakin inkişaf etmiş ölkələrin müqaviməti nəticəsində BTİ tərəfindən bu məqsədlə qəbul edilən D.50 saylı Qətnamə nəticəsiz qaldı.

8. SPAMLARLA MÜBARİZƏ PROBLEMLƏRİ

İnternetin tənzimlənməsi sahəsində meydana çıxan ən mühüm problemlərdən biri də spamlarla mübarizə məsələsidir. Spam – kommersiya, siyasi və digər xarakterli reklamın, yaxud başqa növ məlumatların onları qəbul etmək istəməyən şəxslərə kütləvi göndərişidir [1].

Birincisi, spam – elektron məktubu qəbul edənin əvvəlcədən (ilkin) razılığını almadan (*"unsolicited"*) göndərilən məlumatdır.

İkincisi, göndərişlər kütləvi xarakter daşıyır, yeni bir məlumat eyni zamanda çoxlu sayda elektron poçt ünvanına göndərilir (bir sıra ölkələrdə bu xüsusiyyəti bildirmək üçün *"bulk"* (ing. – "kütlə") terminindən istifadə edilir).

Hər bir kəsin İnternetdəki elektron poçt ünvanına spam göndərilir. Bəziləri bunu qaçılmaz sayır və naməlum şəxs tərəfindən göndərilən məktubu sakitcə silir, digərləri hövsələdən çıxır və məktubu göndərənə, yaxud provayderə öz narazılığını bildirir. Elələri də var ki, göndərilən hər məktubu diqqətlə oxuyur və hətta hərdən onlardan öz xeyri üçün istifadə edir. Göstərilən bütün tip şəxslər İnternetdən, elektron poçtdan istifadə ilə bağlı olan və müəyyən xüsusiyyətlər daşıyan ictimai informasiya münasibətlərinin iştirakçılarıdır.

Spamla göndərilən məlumat spammerin məqsəd və vəzifələrindən asılı olaraq ya kommersiya, ya da qeyri-kommersiya xarakterli ola da bilər. Bu əlamətlərinə görə spamlar iki növə bölünür: kommersiya spamı (*"unsolicited commercial e-mail" - UCE*) və qeyri-kommersiya spamı (*"unsolicited bulk e-mail" - UBE*).

Kommersiya spamlarına, əsasən, reklam məqsədilə göndərilən elektron məktublar aiddir.

Qeyri-kommersiya xarakterli spamlardan, adətən, ictimai tədbirlərin keçirilməsi, siyasi təbliğat və pornoqrafik materialların yayılması üçün istifadə edilir.

Spamlarla mübarizə hər bir istifadəçiyə aidiyyəti olan İnternetin tənzimlənməsi problemlərindən biridir. Virus, spam və haker hücumlarmdan müdafiə sisteminin qabaqcıl istehsalçısı olan *Kaspersky Lab.* şirkətinin 2009-cu ilin 3-cü rübünə (oktyabrın 1-ə) dair təqdim etdiyi hesabata görə, bütün dünya üzrə elektron poçt məktublarının 85,7%-i spam xarakterlidir [35]. Spamın göndərildiyi ölkələr arasında, gözlənildiyi kimi, ABŞ "liderdir". Bu siyahıda Braziliya ikinci, Hindistan üçüncü yerdədir. Spamların 18,8 %-i təhsil, 17,3 %-i dərman preparatları və tibbi xidmətlər, 10,1 %-i spammer xidmətləri, 9,5 %-i istehlak malları, 6,9 %-i səyahət və istirahətlə bağlı reklam materiallarından ibarətdir.

Sual ortaya çıxır ki, nəyə görə spamlarla mübarizə aparılır? Cavabı belədir:

- birincisi, elektron poçt istifadəçiləri spamları qəbul etmələrinə sərf etdikləri vaxta görə provayderlərə pul ödəməli olurlar.
- ikincisi, spamlar kütləvi şəkildə göndərildiyinə görə, informasiya sistemləri və resurslarını lazımsız olaraq yükləməklə, onların fəaliyyətini çətinləşdirir.
- üçüncüsü, spamlarda çox vaxt onu qəbul edəni aldadan məlumatlar olur və bütün bunlar qanunsuz məqsədlərə xidmət edir.

Əgər spamın göstərilən birinci və üçüncü neqativ təsirini qiymətləndirmək çox çətindirsə, ikinci halda mənfi təsiri provayderlər hamıdan yaxşı hiss edirlər. Belə ki,

razılaşdırılmamış məktublar məhz onların sistem və resurslarından istifadə etməklə göndərilir və qəbul edilir.

Spamla həm texniki, həm də hüquqi vasitələrlə mübarizə aparmaq olar. Texniki baxımdan, məlumatları süzgəcdən keçirən və spamları silən bir çox proqramlar mövcuddur. Filtirasiya sistemlərinin əsas problemi ondan ibarətdir ki, onlar bəzən spam olmayan məlumatları da pozur. Spama qarşı mübarizə sənayesi inkişaf edən sektora çevrilib, bu istehsal sahəsində spamı adi poçtdan fərqləndirməyə kömək edən daha mürəkkəb mexanizmlər işlənib hazırlanır. Amma texniki metodlar yalnız məhdudlaşdırıcı təsir göstərir, onlardan istifadə konkret hüquqi mexanizmlərlə müşaiyət olunmalıdır.

Spamlarla mübarizədə ən böyük töhfəni provayderlər verirlər. Onlar bu məqsədlə xüsusi sistem və resurslar hazırlamaq imkanına malikdirlər. Provayderlərin müştəriləri də spamlarla mübarizə apara bilərlər: həm provayderlərə spamlarla bağlı şikayət etməklə, həm də xüsusi müştəri proqram təminatlarını tətbiq etməklə.

Provayderlər spamlarla mübarizə məqsədilə, ilk növbədə, filtirasiya (poçt məlumatlarının seleksiyası və məhv edilməsi) və bloklama (identifikasiya və məlumatlarm qəbulundan imtina etmə) kimi üsullardan istifadə edirlər. Onlar həmçinin özünütənzimləmə mexanizmlərindən istifadə etməklə bir-birləri ilə birləşirlər və birgə təşkilati-texniki fəaliyyət göstərməklə kütləvi poçt göndərişləri və spammerlərlə mübarizənin səmərəliliyini artırmağa cəhd göstərirlər.

Bir sıra ölkələr spamların ictimai təhlükəliliyini dərk edərək, kommersiya və ya qeyri-kommersiya xarakterli razılaşdırılmamış kütləvi poçt göndərişlərini məhdudlaşdıran, yaxud qadağan edən qanunlar qəbul ediblər.

Bu sahədə ABŞ daha fəaldır [1]. Bu ölkədə elektron poçtdan reklam üçün qanuni istifadə ilə spam arasında incə sərhədi tapmağa cəhd etmək üçün *Can-Spam Act* adlanan qanun tətbiq edilir. Qanun spamı yaymağa görə 5 il müddətinə azadlıqdan məhrumetmə kimi ciddi cəza nəzərdə tutsa da, bu hüquqi aktı tənqid edənlər də var. Onların fikrincə, bu qanun spama qarşı olduqca "səbrlidir" və hətta onun yayılmasına şərait yaradır. Qanunda nəzərdə tutulduğuna görə, spama, onu qəbul edənin buna etirazı yoxdursa, icazə verilir. Statistika təsdiq edir ki, həmin qanunun qəbul edildiyi tarixdən – 2003-cü ilin dekabrından sonra ölkədə spamların azalması müşahidə edilməyib.

Birləşmiş Ştatların qanunvericiliyini təhlil edərək, belə qənaətə gəlmək olar ki, hazırda poçt göndərişlərinin tənzimlənməsində daha çox kommersiya spamlarına diqqət yetirilir, provayderlər, adətən, öz istifadəçilərinə göstərdikləri xidmətlərlə əlaqədar toxunulmazlıq hüququna malikdirlər, qanunların pozulmasına görə onlar yalnız mülki məsuliyyətə cəlb edilə bilərlər.

2003-cü ilin iyun ayında Avropa Birliyində spamla mübarizə haqqında xüsusi qanun qəbul edilib [36]. Həmin təşkilatın 2003-cü ilin sonuna qədər bu qanunun tətbiq edilməsi barədə iştirakçı ölkələr qarşısında tələb qoymasına baxmayaraq, 9 ölkə bu müddətə riayət etmədi. Bu qanun spamla mübarizə məsələsində özünütənzimləməyə və özəl sektorun təşəbbüslərinə üstünlük verir.

Norveçdə isə informasiyanı qəbul edənin ilkin razılığı olmadan elektron poçtan istifadəyə əsaslanan "*direct marketing*" fəaliyyəti qadağan edilib. Finlandiyada 1999-cu ildən qüvvədə olan qanuna görə, informasiyanı yalnız

əvvəlcədən onu imzalayan fiziki şəxslərə kütləvi şəkildə göndərilməsinə icazə verilir, əgər hüquqi şəxslərə əvvəlcədən razılaşdırılmayan kommersiya informasiyası göndərilərsə, həmin şəxslərin bundan imtina etmək imkanı olmalıdır [35].

Avstriyada "Telekommunikasiyalar haqqmda" qanuna edilən düzəlişlər razılaşdırılmamış poçt göndərişini qəbul edən şəxsə onu göndərəndən 500 000 Avstriya şillinqi məbləğində cərimə tələb etmək hüququ verir. İtaliyada isə analoji hərəkətə görə 500 avrodan 5 000 avroya qədər kompensasiya nəzərdə tutulur [35].

Avstraliyada 2004-cü ildə qəbul olunan spamla mübarizə haqqında qanun müvafiq qanun pozucularının sərt şəkildə cəzalandırılmasını nəzərdə tutur. Bu qanuna uyğun olaraq, 2006-cı ildə Avstraliya məhkəməsinin qərarı ilə bu ölkənin *Clarity1* şirkəti milyonlarla qeyri-legitim poçt göndərişlərinə görə 4,1 milyon ABŞ dolları məbləğində cərimə ödəməli oldu [36].

Spamla mübarizə məqsədilə ABŞ-da və Avropa Birliyində qəbul edilən qanunların bir zəif yeri var: transmilli spamın qarşısını almaq üçün tədbirlər nəzərdə tutulmayıb. Bu problem Kanada üçün daha aktualdır. Belə ki, statistik məlumatlara görə, bu ölkədə hər 20 spamdan 19-u xaricdən göndərilir. Ona görə də Kanada rəsmiləri haqlı olaraq hesab edirlər ki, bu problem bir ölkə daxilində həll edilə bilməz. Avropa Birliyinin spamla mübarizəyə dair qanunvericiliyini tədqiq edən Amsterdam Universitetinin İnformasiya Hüququ İnstitutunun mütəxəssisləri də bu qənaətə gəliblər. Onların fikrincə, spamların əksəriyyətinin mənbəyi Avropa Birliyi ölkələrindən kənarda yerləşir, bu da müvafiq

qanunvericiliyin effektliliyini əhəmiyyətli dərəcədə azaldır.

Artıq spamla mübarizə sahəsində beynəlxalq əməkdaşlığa dair Avstraliya, Cənubi Koreya və Böyük Britaniya arasında anlaşma Memorandumu imzalanıb [5].

Həmçinin ATƏT tərəfindən Spam üzrə İşçi qrupu yaradılıb və spamla mübarizə üzrə "alətlər dəsti" hazırlanıb. Beynəlxalq Telekommunikasiya İttifaqı da bu məsələ ilə bağlı fəal mövqe nümayiş etdirir. Bu qurum tərəfindən təşkil edilən beynəlxalq müşavirədə (7 iyul 2004-cü il) spama qarşı mübarizə sahəsində qlobal qarşılıqh anlaşma memorandumunun imzalanmasına dair müxtəlif variantlar müzakirə edilib. Regional səviyyədə - Avropa Birliyində Spamla mübarizə sahəsində tədbirlərin həyata keçirilməsi üzrə agentliklər Şəbəkəsi yaradılıb [35].

Spamla beynəlxalq miqyasda mübarizə aparmaq üçün daha bir təşəbbüs elektron poçt xidməti göstərən dünyanın aparıcı İnternet şirkətləri tərəfindən göstərilib. *America Online, British Telecom, Comcast, EarthLink, Microsoft* və *Yahoo* kimi şirkətlər Spama qarşı mübarizə üzrə texniki Alyans (*ASTA*) yaradıblar. Bu alyansın vəzifəsi spamla mübarizə sahəsində texniki və siyasi təşəbbüsləri koordinasiya etməkdir.

Spamın mahiyyəti ilə bağlı fərqli fikirlərin mövcud olması onunla mübarizənin effektliliyinə mənfi təsir göstərir. ABŞ-da söz azadlığının müdafiəsinə həssas yanaşma və Konstitusiyaya birinci düzəliş spamla mübarizəni ləngidir. Amerika qanunvericiləri yalnız "razılaşdırılmamış kommersiya məlumatlarını" spam hesab edirlər, spamların digər növlərini (siyasi təbliğat, pornoqrafik materiallar) bu kateqoriyaya aid etmirlər [26].

Lakin ölkələrin çoxunda məzmunundan asılı olmayaraq, istənilən razılaşdırılmamış məlumat spam hesab edilir. Spamların böyük hissəsinin mənbəyi ABŞ olduğuna görə, bu sahədəki fikir ayrılığı spamla mübarizə sahəsində istənilən effektli beynəlxalq mexanizmlərin yaradılması imkanını əhəmiyyətli dərəcədə məhdudlaşdırır.

Spamın strukturunun ilkin şərtlərindən biri elektron məlumatın saxta ünvandan göndərilməsi imkanıdır. Bu problemin həlli üçün texniki imkanlar mövcuddur. Bu saxtakarlığın reallaşdırılması üçün elektron poçtun mövcud standartlarmm dəyişdirilməsi tələb edilir. IETF elektron məlumatın doğruluğunun müəyyən edilməsinə qarantiya verə biləcək elektron poçt protokoluna dəyişikliklərin tətbiq edilməsi üzərində işləyir. Bu, texniki məsələlərin (standartların) siyasətə təsir etməsi imkanını göstərən faktlardan biridir. Elektron məlumatların doğruluğunun təmin edilməsi üçün vacib olan məsələ İnternetdə anonimliyin məhdudlaşdırılmasıdır.

Göstərildiyi kimi, spamların böyük hissəsi xaricdən göndərilir. Bu, beynəlxalq miqyasda həll olunması tələb edilən qlobal problemdir. Müəyyən təşəbbüslər var ki, onlar bu sahədə qlobal əməkdaşlığın səmərəliliyinin yüksəldilməsinə gətirib çıxara bilər. Qarşılıqlı anlaşmaya dair ikitərəfli memorandumların imzalanması bu istiqamətdə atılan ilkin addımlardan biridir. Problemlə daha səmərəli və geniş həcmdə mübarizə aparmaq üçün qlobal səviyyədə təsir mexanizmlərinin işlənib hazırlanmasına ehtiyac var.

Hələlik inkişaf etmiş ölkələr milli qanunvericiliklərini möhkəmləndirmək yolu ilə və paralel olaraq ikitərəfli və ya regional əməkdaşlıq çərçivəsində mübarizə aparmağa

üstünlük verirlər. İnkişaf etməkdə olan ölkələr isə, spam qəbulediciləri kimi öz əlverişsiz vəziyyətlərini nəzərə alaraq, bu problemlə qlobal miqyasda mübarizə aparmaqda maraqlıdırlar.

İnkişaf etmiş ölkələrin istifadəçiləri, çətinliklə də olsa, spamların yaratdığı çətinliklərin öhdəsindən gələ bilirlər. Bir çox inkişaf etməkdə olan ölkələrdə isə spam bütün İnternet infrastrukturuna ciddi ziyan vurur. Həmin ölkələrdə məlumatlarm aşağı sürətlə ötürüldüyü və İnternet infrastrukturunun inkişaf etmədiyi bir şəraitdə spam istifadəçilərin bu qlobal şəbəkəyə çıxışında ciddi problem yaradır. Bu tip ölkələrdə spamla mübarizə üçün texniki resurslar və biliklər çatışmır. Bununla da, spam inkişaf etmiş və inkişaf etməkdə olan ölkələr arasındakı rəqəmsal uçurumu daha da dərinləşdirir

9. İNTELLEKTUAL MÜLKİYYƏT HÜQUQLARININ QORUNMASI PROBLEMLƏRİ

Bilik və ideyalar qlobal iqtisadiyyatda mühüm resursa çevrilir. Onların əqli mülkiyyət hüququ formasında qorunması İnternetin tənzimlənməsinin ən vacib məsələlərindən biri kimi çıxış edir. Əqli mülkiyyət hüquqlarının qorunması ilə bağlı məqamlar İnternetin tənzimlənməsinin müxtəlif aspektləri ilə əlaqədardır. Belə ki, bilik və ideyalar mədəni irsin və sosial münasibətlərin mühüm tərkib hissələri kimi, bir çox cəmiyyətlər üçün xüsusi dəyərə malikdir. Əqli mülkiyyət hüququ həmçinin İnternetin inkişafı ilə bağlı disskussiyaların əsas mövzularından biridir.

Şübhəsiz ki, cəmiyyətin maraqları baxımından, İnternetdə ədəbiyyat, incəsənət əsərləri, filmlər, proqram təminatı və verilənlər bazası nə qədər çox olarsa, bir o qədər yaxşıdır. Çünki İnternet texnologiyaları və xidmətləri operativ şəkildə və minimal xərclər hesabına həmin mənbələri nəhəng istifadəçi auditoriyasına təqdim edə bilir ki, bu da şəxsiyyətin və cəmiyyətin inkişafına xidmət edir. Lakin tez-tez bu və ya digər materialların İnternetdə yerləşdirilməsi müəllif hüquqlarını pozur, yaxud buna şərait yaradır. Beləliklə, informasiya mübadiləsi azadlığı müsbət tərəfləri ilə yanaşı, neqativ nəticələrə də yol açır.

Əqli mülkiyyətin əsasını müəllif hüquqları, patentlər və əmtəə nişanları təşkil edir. Eyni qaydada, İnternetdə də əqli mülkiyyət hüququ ilə bağlı problemləri bu cür qruplaşdırmaq olar [37].

Müəllif hüquqları

Müəllif hüququ – mülki hüququn elm, ədəbiyyat və ya incəsənət məhsulunun yaradılması və istifadəsi (nəşri, ifası, nümayişi) ilə bağlı hüquq münasibətlərini tənzimləyən bir sahəsidir. Müəllif hüququnun əsasında "yaradıcılıq" anlayışı və ya hər hansı obyektiv formada mövcud olan yaradıcılıq fəaliyyətinin orijinal nəticəsi dayanır. Məhz bu obyektiv ifadə forması müəllif hüququnda müdafiə predmeti kimi çıxış edir [38].

Müəllif hüququnun obyektləri – dəyərindən və təyinatından, həmçinin ifadə formasından asılı olmayaraq elm, ədəbiyyat və incəsənət sahəsində yaradıcılıq məhsuludur.

Müəllif hüququnun subyektləri – elm, ədəbiyyat və incəsənət sahəsində yaradıcılıq məhsuluna dair müstəsna hüquqları olan şəxslərdir. Yəni həmin məhsulu yaradanlar onun müəlliflərıdir.

Mətn hissələrini "kəsmək" və "əlavə etmək" imkanlarından başlamış, audio-video faylların virtual mühitdə yayılmasına kimi mürəkkəb əməliyyatlara qədər İnternet texnologiyalarının inkişafı ənənəvi müəlliflik hüququ konsepsiyasını zərbə (təhlükə) qarşısında qoydu. İnternet vasitəsilə cüzi xərclər hesabına müxtəlif materialları köçürmək və bütün dünyaya yaymaq imkanı yarandı [5].

Bu imkanlar material müəlliflərinin maraqları və cəmiyyətin yaradıcılıq fəaliyyətinə, ictimai biliklərə marağı arasındakı kövrək tarazlığı təhlükə altında qoyur. Materialların məhdudiyyətsiz köçürülməsinin qarşısının alınması və eyni zamanda, həmin materiallardan istifadə imkanının saxlanılması İnternetin tənzimlənməsi ilə bağlı

ən çox baş sındırılan məsələlərdən biridir. Bu gün maraqları iri səsyazma və multimedia şirkətləri tərəfindən təmsil edilən müəlliflik hüquqlarının sahibləri öz hüquqlarını daha fəal şəkildə qoruya bilirlər, nəinki sıravi istifadəçilər. İctimai maraqlar isə hələ kifayət qədər dəqiq formalaşmayıb və lazımi səviyyədə qorunmur.

Patent

Patent - ixtira, faydalı model və sənaye nümunəsi üçün müvafiq səlahiyyətli dövlət orqanı tərəfindən verilən mühafizə sənədidir. Ənənəvi anlamda patent – başlıca olaraq, texniki və istehsal sahəsində yeni prosesi və ya məhsulu müdafiə edir. Artıq proqram təminatı vasitələri də patent hüquqlarının obyekti kimi çıxış edir. Qeydiyyatdan keçmiş patentlərin sayının sürətlə artması böyük pullarla bağlı olan və Amerikanın proqram təminatı istehsalçılarının iştirakı ilə keçirilən məhkəmə işlərinin həcmini də artırır [38].

İnternetin tənzimlənməsi nöqteyi-nəzərincə, əsas problem qlobal şəbəkədə biznes proseslərinin patent müdafiəsi ilə bağlıdır. Bu problemə misal olaraq *Amazon* şirkəti tərəfindən istifadə edilən "siçanı" bir dəfə sıxma ("*1-Click*") prosedurunu göstərmək olar. Həmin məsələ ilə bağlı problem ondan ibarət idi ki, *Amazon* konkret biznes prosesini (alış prosedurunu) yox, yalnız ideyanı (bir dəfə sıxmadan istifadəni) patentləşdirib [5].

"1-Click" proseduruna görə patentin uğurla qeydiyyatı böyük bir patent ərizələri dalğası yaratdı. Hətta bəzi gülüş doğuran cəhdlər də oldu. Məsələn, İnternetdən faylların yüklənməsinə görə patent almaq istəyənlər ortaya çıxdı. *British Telecom*-un 1980-ci ildə qeydiyyatdan

keçirdiyi hipermətn istinadı üzrə patentinə görə lisenziya haqqı tələb etməsi isə heç də sadə məsələ deyildi. Şirkət bu istəyinə nail olsaydı, İnternet istifadəçiləri yaratdıqları və ya istifadə etdikləri hər bir istinada görə pul ödəməli olacaqdılar.

Qeyd etmək vacibdir ki, İnternet prosedurları ilə bağlı olan proqram təminatı məhsullarına patentlərin verilməsi məsələsi Avropa Birliyi və dünyanın əksər ölkələri tərəfindən dəstəklənmir.

İnternetdə intellektual mülkiyyət hüquqlarının qorunması probleminə qarşı mübarizə kompleks xarakter daşımalıdır. Bu, aşağıdakılarla əlaqədardır [37]:

- müvafiq hüquq pozuntuları təkcə İnternetdə yox, həm də digər İKT vasitələrində baş verir;
- bu vasitələrdən istifadə etməklə aşağıdakı hüquq pozuntuları törədilir: plagiatlıq; əqli mülkiyyət hüququ obyektləri ilə qanunsuz ticarət; İnternet-mağazalar vasitəsilə icazəsiz məhsulların alqı-satqısı;
- ən müxtəlif əqli mülkiyyət hüququ obyektləri müvafiq qanun pozuntularının obyekti kimi çıxış edir;
- müvafiq qanun pozuntuları transmilli (qlobal) xarakter daşıyır;
- müvafiq qanun pozuntuları bir çox hallarda digər ictimai-təhlükəli əməllərlə - ziyanlı proqramların, spamların yayılması, fərdi məlumatların işlənmə qaydasının pozulması və s. ilə müşahidə olunur.

İntellektual mülkiyyət hüquqlarının qorunması üsullarından biri texniki tədbirlərə əsaslanır [39]. Bu müdafiə metodu Stokholm Konvensiyasının 11-ci maddəsində öz əksini tapıb. Həmin maddədə müəllif hüquqlarının və əlaqəli hüquqların qorunması məqsədilə texniki tədbirlərin görülməsi tövsiyə edilir. Belə bir müddəa Avropa Birliyinin 22 may 2001-ci il tarixli "İnformasiya cəmiyyətində müəllif və əlaqəli hüquqların ayrı-ayrı aspektlərinin harmoniyalaşdırılması haqqında" Direktivində də qeyd edilir. Bu Direktivadə Stokholm Konvensiyasında göstərilən ideya daha da inkişaf etdirilir. Belə ki, Direktivdə müvafiq texniki tədbirlərə riayət etməmək qadağan edilir.

Əqli mülkiyyət hüquqlarının qorunması yollarından biri də İnternet-provayderlərin üzərinə müvafiq məsuliyyətin qoyulmasıdır. Bu metod beynəlxalq əhəmiyyətə malikdir. Çünki İnternet sərhəd tanımır. Ona görə də müvafiq problemin həlli üçün bu metodun beynəlxalq səviyyədə tətbiqi vacibdir.

Avropa Birliyinin Elektron Kommersiya üzrə Direktivində texniki kopyalama (keşləşdirmə) üzrə fəaliyyətlə əlaqədar məsuliyyətə görə istisnalar müəyyən edilib [36]. O cümlədən İnternet-provayderlər bu cür surətçıxarmanı həyata keçirərkən ötürülən informasiyanın məzmununu dəyişdirməməlidirlər, yaxud ötürülən informasiyanın məzmununun qeyri-qanunu olduğunu bildikdə, bu cür informasiyadan istifadənin qarşısının alınması üçün vaxtında tədbir görməlidirlər.

Əmtəə nişanları

Əmtəə nişanı – hər hansı bir sahibkarın əmtəələrini və ya xidmətlərini digər sahibkarın əmtəələrindən və ya xidmətlərindən fərqləndirən və qrafik formasında təsvir edilən nişan və ya nişanların hər hansı bir uzlaşmasıdır (kombinasiyasıdır) [40].

Əmtəə nişanlarının qorunması sahəsində başlıca problem domen adlarının qeydiyyatının tənzimlənməsi ilə bağlıdır. İnternetin inkişafının ilkin mərhələlərində domen adı ərizə ilə birinci müraciət edənə verilirdi. Bu, praktikada "kiberskvottinq" adlanan fəaliyyətin, yəni şirkət adlarının domen adı qismində qeydiyyatdan keçirilməsinə və sonra onların yüksək qiymətə satılması hallarının artmasına gətirib çıxartdı. İnternetin yayılması və iqtisadi potensialının artması nəticəsində həmin məsələ ciddi problemə çevrildi. Çünki artıq domen adları şirkətlərin reputasiyasına təsir etməyə başlayırdı. Vəziyyətin ənənəvi məhkəmə sistemləri vasitəsilə hüquqi metodlarla həlli məqsədəuyğun deyildi. Çünki bu cür məsələlərə baxmaq olduqca çox vaxt aparırdı.

Müvafiq situasiya biznes sektorunu əmtəə nişanlarının müdafiəsi ilə bağlı İnternetin idarə edilməsi üzrə islahat Mərkəzi qarşısında məsələ qaldırmağa vadar etdi ki, bu da, öz növbəsində, *ICANN* adlanan təşkilatın yaradılmasına gətirib çıxartdı. ABŞ hakimiyyətinin hazırladığı "Ağ kitab"da *ICANN*-a domen adları sahəsində əmtəə nişanlarının qorunması mexanizmlərinin işlənib hazırlanması və tətbiq edilməsi vəzifəsi həvalə edildi [3].

10. KİBERCİNAYƏTKARLIQLA MÜBARİZƏ PROBLEMLƏRİ

Texnologiya fayda vermək üçün yaradılır, amma ondan bir sıra hallarda qeyri-qanuni, cinayət məqsədləri üçün də istifadə edilir. İKT sahəsində, o cümlədən İnternet mühitində həyata keçirilən hüquq (qanun) pozuntuları ümumi şəkildə "kibercinayətkarlıq" termini ilə ifadə olunur. Eyni zamanda, "cinayətkarlıq" termini kifayət qədər aydın şəkildə müəyyən edilsə də (məsələn, böhtan, uşaq pornoqrafiyası), "kiber" anlayışı ilə bağlı müxtəlif yanaşmalar mövcuddur [5].

"Real" və "virtual" hüquq arasında fərqlər bu sahədə də özünü göstərir. "Real" hüquq tərəfdarları qeyd edirlər ki, kibercinayətkarlıq – gerçək dünyada da məlumdur, sadəcə, kompyuterin köməyi ilə həyata keçirilir. Cinayətkarlıq olduğu kimi qalır, yalnız vasitələr dəyişir. "Kiber" hüquq tərəfdarları isə hesab edirlər ki, kibercinayətkarlığın unikal elementləri ona xüsusi yanaşma tələb edir, o cümlədən qanunların tətbiqi və cinayətkarlığın profilaktikasında bunu nəzərə almaq lazımdır.

BMT ekspertlərinin tövsiyələrinə əsasən, "kibercinayətkarlıq" termini kompyuter sistemlərinin və şəbəkələrinin köməyi ilə, yaxud kompyuter sistemlərinə və şəbəkələrinə qarşı həyata keçirilən istənilən cinayət əməlini əhatə edir [41]. Başqa sözlə desək, virtual mühitdə həyata keçirilən istənilən cinayət növünü "kibercinayət" adlandırmaq olar.

Kibercinayətkarlıq əməllərini iki qrupa bölmək olar: yalnız kiberməkana xas olan cinayətlər və kompyuter və İnternet vasitəsilə həyata keçirilən ənənəvi cinayətlər [42].

Yalnız kiberməkana xas olan cinayət əməllərinə aşağıdakıları aid etmək olar:

- kompyuter informasiyasına qanunsuz daxilolma;
- kompyuter və İnternet üçün ziyanlı proqramların yaradılması, istifadəsi və yayılması;
- kompyuterin və informasiya sistemlərinin normal fəaliyyətinin pozulması (kompyuter sabotajı);
- xüsusi təyinatlı radioelektron sistemlərin qanunsuz dövriyyəsi;
- kompyuter vasitəsilə elektron sənədlərin saxtalaşdırılması;
- lisenziyalaşdırılmamış proqram təminatının yayılması;
- İnternetdə maliyyə fırıldaqçılığı və saxtakarlığı;
- İnternet casusluğu
- kiberdələduzluq

İnternet vasitəsilə həyata keçirilən ənənəvi cinayətlərə bunlar aiddir:

- həyat və sağlamlıq əleyhinə olan cinayətlər;
- şəxsiyyətin azadlığı, şərəf və ləyaqəti əleyhinə olan cinayətlər;
- yetkinlik yaşına çatmayanlara qarşı cinayətlər;
- mülkiyyət əleyhinə cinayətlər;
- iqtisadi sahədə cinayətlər;
- ictimai təhlükəsizlik əleyhinə olan cinayətlər;
- əhalinin sağlamlığına və ictimai əxlaqa qarşı cinayətlər;

- konstitusiya quruluşu və dövlət əleyhinə cinayətlər;
- pornoqrafiyanın yayılması;
- narkobiznes;

Kibercinayətkarlığın ən xarakterik xüsusiyyətləri bunlardır:

- qeyri-aşkarlığı;
- istintaqının həddindən artıq mürəkkəbliliyi;
- vurduğu ziyanın böyük həcmli olması;
- milli sərhədlərin kibercinayətkarlar üçün şəffaflığı;
- bu sahədə mübarizə üçün hüquqi bazanın zəif olması;
- kibercinayətkarların yüksək ixtisaslı peşəkarlardan ibarət olması.

Kibercinayətkarlığın yaranma tarixi, təxminən, İnternetin yaranma tarixi ilə eynidir [43]:

- Artıq ötən əsrin 70-ci illərində "haker" termini meydana gəldi. Sonradan bu termin bütün kompyuter və İnternet cinayətlərinə şamil edilməyə başladı.
- 1983-cü ildə ilk dəfə olaraq ABŞ-ın Miluoki ştatında İnternet-cinayətkar həbs edildi. Ümumiyyətlə, ötən əsrin 80-ci illərində kibercinayətlərin sayının artması müşahidə edilməyə başlayır.
- 1984-cü ildə ABŞ-ın Cənubi Kaliforniya Universitetinin tələbəsi Fred Koen "kompyuter virusu" adlandırdığı ilk özüçoxalan ziyanlı kompyuter proqramını nümayiş etdirdi.

- 1986-cı ildə ABŞ-da kompyuter sistemlərinə qanunsuz daxilolmanı və məxfi hərbi informasiyanı əldə etməyi qadağan edən ilk kompyuter qanunu qəbul olundu.
- 1994-cü ildə Sankt-Peterburqda kompyuter proqramçısı Vladimir Levin qanunsuz yolla Nyu-Yorkdakı *Citibank*-ın kompyuter şəbəkəsinə daxil olaraq 12 milyon dolları ələ keçirdi. Bu ilk taransmili kompyuter cinayəti kimi bütün dünyada əks-səda doğurdu.
- 2002-ci ildə bütün İnternet infrastrukturunun işinin dayandırılmasına yönələn hücum həyata keçirildi. Bundan sonra İnternet-cinayətkarlığm qloballaşma problemi daha da genişlənməyə başladı.

Ümumiyyətlə, İnternet-cinayətkarlığın inkişaf tarixini dörd mərhələyə bölmək olar [43]:

1. İnternetin qlobal şəbəkə kimi meydana gəlməsi. Həmin vaxtlar İnternet-cinayətkarlıq hələ aktuallıq kəsb etmirdi. Yalnız ayrı-ayrı əməllər ictimai təhlükə yaradırdı.
2. İnternet-cinayətkarlığm meydana gəlməsi. Bu mərhələdə hakerlik fəaliyyəti yaranır, İnternetdə cinayətlərin sayı artır. Həmin vaxtlar İnternet-cinayətkarlıq yalnız məhdud mütəxəssislər dairəsində həyata keçirilirdi. Kompyuter cinayətləri sahəsində ixtisaslaşma gedirdi.
3. İnternetdən ənənəvi cinayətlərin həyata keçirilməsi üçün istifadə edilməyə başlanılır. Ayrı-ayrı ölkələrdə İnternet-cinayətkarlıq

geniş yayılır, böyük milli "haker qrupları" meydana gəlir.

4. İnternet-cinayətkarlıq artıq transmilli (qlobal) xarakter daşımağa başlayır. Kiberterrorizm, beynəlxalq haker qruplaşmaları meydana gəlir. İnternetdə transmilli cinayətlərin sayı artır. Qlobal şəbəkədən İnternet-iğtişaş, İnternet-müharibə kimi siyasi məqsədlər üçün istifadə edilməyə başlanılır.

Kriminal faktlara dair statistik məlumatların təhlili də göstərir ki, kibercinayətkarlıq halları digər analoqları ilə müqayisədə daha sürətlə artmaqdadır. Ekspertlər bunun əsas səbəbi kimi cinayətkarların minimal risk hesabına vətəndaşlara və təşkilatlara daha çox maliyyə ziyanı vurmaq imkanını göstərirlər.

Artıq İnternet-cinayətlərin ənənəvi cinayət hallarını üstələyəcəyi, iqtisadi və siyasi proseslərə daha geniş şəkildə təsir edəcəyi proqnozlaşdırılır. Uğurlu tənzimləmə və mübarizə siyasətinin həyata keçiriləcəyi halda, İnternet-cinayətkarlığın artım tempinin aşağı salınması da istisna edilmir.

İnternet-cinayətkarlıqla mübarizə sahəsində hüquqi tənzimləmə prosesinin inkişafını dörd mərhələyə bölmək olar [43]:

1. İnternet və kompyuter sahəsində heç bir qanunvericilik norması mövcud deyil. Bu vaxt İnternet vasitəsilə həyata keçirilən cinayətlərə görə mövcud ənənəvi hüquq normalarının analogiya üzrə tətbiqinə cəhdlər edilir.
2. Kompyuter və İnternet cinayətlərinin sayının artmasına cavab olaraq bu sahəyə aid ilk xüsusi qanun və hüquq normaları yaradılır.

3. Kibercinayətkarlıq sahəsindəki qanunvericilik artıq ayrıca hüquq sahəsinə çevrilir. İnternet-cinayətkarlıq hallarının kəskin şəkildə artmasına cavab olaraq müvafiq hüquqi sanksiyalar da sərtləşdirilir.
4. Kibercinayətkarlığın beynəlxalq miqyas alması ilə əlaqədar İnternetlə bağlı ictimai münasibətləri tənzimləyən beynəlxalq hüquq normaları meydana gəlir.

Kibercinayətkarlıqla hüquqi müstəvidə mübarizəyə başlanması 2000-ci illərin əvvəllərinə təsadüf edir. Beynəlxalq təşkilatlar ayrı-ayrı dövlətlərə tövsiyə edirlər ki, öz cinayət qanunvericiliklərinə kibercinayətlər haqqında xüsusi müddəalar əlavə etsinlər. O cümlədən BMT-nin Baş Assambleyası tərəfindən bu istiqamətdə bir neçə qətnamə qəbul edilir. Həmçinin 2003-cü ildə ATƏT İnternet dələduzluğu ilə mübarizədə dövlətlərə kömək etmək məqsədilə müvafiq sahə üzrə əsas prinsiplər hazırlamır [27].

2003-cü ildə Budapeştdə Avropa Şurası tərəfindən imzalanan Kibercinayətkarlıq haqqında Konvensiya isə hələlik müvafiq sahədə ən mühüm sənəd kimi çıxış edir [6]. Bu Konvensiyaya qoşulan dövlətlər müvafiq qanunvericilik aktlarının qəbul edilməsi ilə və beynəlxalq əməkdaşlığın möhkəmləndirilməsi vasitəsilə cəmiyyəti kibercinayətlərdən qorumaq məqsədi daşıyan cinayət hüququ sferasında ümumi siyasətin aparılması barədə öhdəlik götürürlər. Bu beynəlxalq müqavilə İnternet infrastrukturunun cinayət əməllərindən qorunması üzrə ümumi prinsiplərin hazırlanmasına yönəlib və qlobal şəbəkə ilə bağlı hüquq pozuntularının məhkəmə istintaqının prosedurunu müəyyən edir.

Konvensiya üzv dövlətlərin aşağıdakı cinayət növlərinin milli səviyyədə qanunvericilik aktlarına daxil edilməsini nəzərdə tutur:

- kompyuter məlumatları və sistemlərinin məxfiliyi, bütövlüyü və istifadəsi ilə bağlı cinayətlər;
- kompyuter vasitələrindən istifadə yolu ilə həyata keçirilən cinayətlər;
- məlumatların məzmunu ilə bağlı cinayətlər;
- müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı hüquq pozuntuları.

Qeyd edək ki, Kibercinayətkarlıq üzrə Konvensiya təhlükəsizlik və insan hüquqları arasında tarazlığa dair disskussiyaları kəskinləşdirdi. Başlıca olaraq, vətəndaş cəmiyyətinin təmsilçiləri narahatdırlar ki, bu konvensiya hakerlərin kompyuterlərini yoxlamaq, informasiya mübadiləsinə nəzarət etmək və s. daxil olmaqla, hakimiyyət orqanlarına həddindən çox səlahiyyətlər verir. Bu geniş səlahiyyətlər müəyyən insan hüquqlarını, o cümlədən şəxsi həyatın toxunulmazlığı və öz etiqadını (əqidəsini) ifadə etmək azadlığını təhlükə qarşısında qoya bilər.

Kibercinayətkarlıqla mübarizədə əsas çətinliklərdən biri məhkəmə işinin aparılması üçün məlumatların toplanmasıdır. Müasir kommunikasiyaların sürəti hüquq-mühafizə orqanları tərəfindən çevik reaksiya tələb edir.

Məlumatların saxlanmasının mümkün üsullarından biri provayderlər tərəfindən elektron protokolların ("loq-faylların") aparılmasıdır. Həmin protokollarda kimin və nə vaxt bu və ya digər resursa daxil olması barədə informasiya daxil edilir. Müvafiq Konvensiyanın bəzi müddəaları bu sahəyə həsr olunub.

"İnternet vasitəsilə irqi, ksenofobiya (yad mədəniyyətə, adət-ənənəyə və s. qarşı dözümsüzlük) və antisemitizm xarakterli materialların yayılmasının qarşısının alınması haqqında" Avropa Birliyi Komissiyasının Ümumsiyasi Tövsiyələri (Strasburq, 15 dekabr, 2000-ci il) də kibercinayətkarlığa qarşı mübarizə baxımından mühüm əhəmiyyət kəsb edir [36]. Bu sənəddə üzv ölkələrə İnternetdə rasizm, ksenofobiya və antisemitizm xarakterli materialların yayılmasına qarşı mübarizə aparmaq, bu sahədə beynəlxalq əməkdaşlığı gücləndirmək, milli qanunvericiliyə müvafiq normaları daxil etmək, hüquq-mühafizə orqanlarını bu cinayət əməllərinə qarşı mübarizə üçün hazırlamaq, əhalini İnternet vasitəsilə müvafiq problem haqqında məlumatlandırmaq və s. tövsiyə olunur.

11. ELEKTRON KOMMERSİYANIN TƏNZİMLƏNMƏSİ PROBLEMLƏRİ

"Elektron kommersiya" anlayışının dəqiq müəyyən edilməsi bir çox praktiki və hüquqi əhəmiyyətə malikdir. Yəni elektron alqı-satqının tanınması halında bu fəaliyyət növünün xüsusi tənzimləmə normaları tətbiq edilir (o cümlədən, vergi və gömrük ödəmələri sahəsində).

Elektron kommersiyanın əsas xüsusiyyətlərindən biri onun hüquqi tənzimlənməsi ilə bağlıdır. Bu sahədə bütün dövlətlər üçün vahid tənzimlənmə siyasətinin həyata keçirilməsi tələb edilir. Çünki milli səviyyələrdə qlobal məkandan təcrid olunmuş hüquqi rejimlərin müəyyən edilməsi beynəlxalq elektron ödənişlərin həyata keçirilməsində hüquqi ziddiyyətlər yaradır.

ABŞ hökumətinin nöqteyi-nəzərincə, elektron ticarəti ənənəvi ticarətdən fərqləndirən əsas meyar on-layn rejimində mal və xidmətləri satmaq öhdəliyidir. Bu o deməkdir ki, on-layn rejimində əldə edilən istənilən kommersiya sövdələşməsi (onun yerinə yetirilməsi malın fiziki olaraq çatdırılmasını nəzərdə tutsa belə) elektron kommersiya sayılır [5]. Məsələn, *Amazon.com* saytı vasitəsilə kitabın əldə edilməsi elektron alqı-satqı sayılır. Baxmayaraq ki, bu halda kitab adi poçtla çatdırılır. ÜTT-nin verdiyi tərifə görə, elektron kommersiya – əmtəə və xidmətlərin elektron üsulla istehsalı, yayılması, reklamı, satışı və çatdırılmasıdır [34].

Elektron kommersiyanın müxtəlif növləri mövcuddur [44]:

- *business-to-consumer (B2C)* – firma tərəfindən əmtəə və xidmətlərin fiziki şəxslərə satışı; Bu, elektron kommersiyanın ən çox yayılmış növüdür (məsələn, *Amazon.com*).
- *business-to-business (B2B)* – firmalar arasındakı ticarət; Bu, elektron kommersiyanın iqtisadi baxımdan ən mühüm növüdür.
- *business-to-government (B2G)* – elektron dövlət satınalmaları; Dövlət satınalmaları siyasəti baxımından elektron kommersiyanın ən mühüm növüdür.
- *consumer-to-consumer (C2C)* – əmtəə və xidmətlərin fiziki şəxslər tərəfindən digər fiziki şəxslərə satışı. Buna misal olaraq, ilk növbədə, elektron hərracları (*eBay* kimi) göstərmək olar.

Bir çox ölkələr elektron kommersiyanın tənzimlənməsi üçün müvafiq hüquqi mühit yaradırlar. Artıq bu məqsədlə elektron imza mübahisələrinin həlli, kibercinayətkarlıq, istehlakçı hüquqlarının qorunması, vergi və s. məsələlərə dair qanunlar qəbul edilib. Beynəlxalq səviyyədə də elektron kommersiyanın tənzimlənməsi ilə bağlı təşəbbüslər artmaqdadır.

Bütövlükdə, elektron kommersiyanın normal fəaliyyətinin və inkişafının təmin edilməsi üçün İnternetin tənzimlənməsi sahəsində aşağıdakı bir sıra məsələlərin həlli vacibdir [45, 46]:

- genişzolaqlı İnternetdən istifadənin və keyfiyyətli xidmətin təmin edilməsi multimedia sahəsində (məsələn, audio-video məhsulların yayılması) elektron kommersiyanın sürətli inkişafının ən vacib şərtlərindən biridir;

- internetin təhlükəsizliyinin təmin edilməsi elektron kommersiya mühitinin etibarlılığını və davamlılığını yüksəltməlidir; Bu, istehlakçıların müvafiq sahəyə etimadının möhkəmləndirilməsi üçün zəruri şərtlərdən biridir.
- informasiyanın şifrələnməsi maliyyə əməliyyatlarının həyata keçirildiyi şəraitdə kommunikasiyaların qorunması üçün olduqca vacibdir;
- yurisdiksiya məsələlərinin həlli elektron kommersiyanın etibarlılığının təmin edilməsi, xüsusən də, istehlakçı hüquqlarının qorunması baxımından vacibdir;
- qeyri-maddi məhsullarla bağlı alqı-satqı əməliyyatlarının həcminin artması ilə əlaqədar əqli mülkiyyət hüququnun qorunması elektron kommersiya üçün xüsusi əhəmiyyət kəsb etməyə başlayır;
- elektron imzadan istifadə alqı-satqı əməliyyatlarının həyata keçirilməsini asanlaşdırır və identifikasiya problemini həll edir;
- elektron kommersiya prosesində alıcılar haqqında çoxlu informasiya toplandığına görə fərdi məlumatların qorunması şəxsi həyatın müdafiəsi baxımından aktuallıq kəsb edir.

Müasir beynəlxalq ticarətdə əsas oyunçu olan ÜTT elektron kommersiya üçün vacib olan bir çox məsələləri, o cümlədən telekommunikasiyaların liberallaşdırılması, əqli mülkiyyət hüquqlarının qorunması və İKT-nin inkişafının bəzi aspektlərini tənzimləyir [34]. ÜTT-nin aşağıda

göstərilən təşəbbüsləri elektron kommersiya ilə bilavasitə əlaqədardır:

- elektron transaksiyaya görə gömrük ödənişlərinin müvəqqəti moratoriumu -ödəmə müddətinin uzadılması (1998-ci il); Buna uyğun olaraq İnternetdə həyata keçirilən bütün sövdələşmələr gömrük ödənişlərindən azad edildi.
- ÜTT-nin elektron kommersiya üzrə İşçi qrupunun yaradılması; Bu İşçi qrupu çərçivəsində elektron kommersiya ilə bağlı problemlərin həlli istiqamətində disskussiyalar aparılır.

Elektron kommersiya sahəsində həllini gözləyən mübahisəli məqamlardan biri də audio-məhsulun alıcıya necə çatdırılmasından (kompakt-diskdə (maddi forma) və ya İnternet vasitəsilə (qeyri-maddi formada)) asılı olaraq onun təsnifatının dəyişib-dəyişməməsi ilə bağlıdır [5]. Son nəticədə eyni audio-məhsul onun alıcıya necə çatdırılmasından asılı olaraq fərqli əmtəə statusu alır və fərqli vergi və gömrük ödənişlərinə cəlb edilir. Bu baxımdan, müvafiq təsnifatın aparılması çox vacibdir, çünki əmtəə və xidmət satışına müxtəlif hüquq normaları tətbiq edilir.

Elektron kommersiya sahəsində ən uğurlu və fəal şəkildə dəstəklənən beynəlxalq təşəbbüslərdən biri də BMT-nin Beynəlxalq Ticarət Hüququ Komissiyasının (YUNİSTRAL) hazırladığı Elektron kommersiya haqqında model qanunudur [47]. Bu sənədin əsas məqsədi elektron və ənənəvi kommersiya qanunvericiliklərinin inteqrasiya mexanizminin hazırlanması və həyata keçirilməsidir.

Müvafiq hüquqi akt bir çox ölkələrin elektron kommersiya üzrə qanunvericiliyinin hazırlanmasının əsasını təşkil edir.

BMT-nin Ticarət və inkişaf üzrə Komissiyası (YUNKTAD) və BMT-nin İKT üzrə Məqsədli Qrupu da elektron kommersiya sahəsində potensialın inkişafına və tədqiqatlara həsr olunmuş müxtəlif tədbirlər həyata keçirir [48].

Biznes sektorunda ən fəal təşkilat kimi elektron kommersiya məsələlərinə dair çoxlu sayda tövsiyələr və analitik hesabatlar hazırlayan Beynəlxalq Ticarət Palatası, habelə milli və beynəlxalq səviyyələrdə elektron kommersiyanın inkişafı üçün səy göstərən Qlobal Biznes-Dialoq çıxış edir [46].

Həmçinin Avropa Birliyi tərəfindən də elektron ticarətin inkişaf strategiyası hazırlanıb (2000-ci il) [36]. Bu strategiyada əsas diqqət özəl və bazaryönümlü təşəbbüslərə yönəldilsə də, dövlət və ictimai maraqların qorunması ilə bağlı məsələlər də öz əksini tapıb. Bundan başqa, Avropa Birliyi tərəfindən Elektron kommersiya üzrə Direktiv, habelə elektron imza, məlumatların müdafiəsi və elektron maliyyə əməliyyatları barədə bir sıra sənədlər qəbul edilib.

Asiya-Sakit okean regionunda elektron kommersiya sahəsində qarşılıqlı əlaqə mərkəzi kimi Asiya-Sakit okean iqtisadi əməkdaşlığı (ASİƏ) fəaliyyət göstərir [49]. Bu qurum çərçivəsində yaradılan Elektron Kommersiya üzrə Rəhbər Qrup müvafiq sahədəki problemləri araşdırır. Bu qrupun ən əhəmiyyətli təşəbbüsü ASİƏ-nin regionda 2010-cu ilə kimi tamamilə kağızsız sənəd dövriyyəsinə əsaslanan ticarət sisteminin yaradılmasına yönələn fəaliyyət planıdır.

İstehlakçı hüquqları

İstehlakçı etimadı elektron kommersiyanın uğurlu inkişafının əsas şərtlərindən biridir. Elektron kommersiya tamamilə yeni fəaliyyət sahəsidir, ona görə də istehlakçılar bu sistemə ənənəvi kommersiya qədər etibar etmirlər. İstehlakçı hüquqlarının müdafiəsi elektron kommersiyaya qarşı etimadın möhkəmləndirilməsində mühüm hüquqi vasitə kimi çıxış edir.

Elektron kommersiyanın tənzimlənməsi istehlakçıları vicdansız reklamdan, keyfiyyətsiz əmtəə və xidmətlərdən, oğurluqdan və şəxsi maliyyə məlumatlarının (məsələn, ödəmə kartları haqqında informasiyanın) qanunsuz ötürülməsindən və s. qorumalıdır [50]. Elektron kommersiyanın yeni səciyyəvi xüsusiyyəti istehlakçı hüquqlarının beynəlxalq səviyyədə qorunması zərurətidir. Halbuki bu xüsusiyyət ənənəvi ticarət üçün prioritet məsələ deyil. Əgər əvvəllər istehlakçılar beynəlxalq müdafiəyə nadir hallarda ehtiyac duyurdularsa, elektron kommersiyanın inkişafının nəticəsi kimi getdikcə daha çox ticarət sövdələşmələri milli sərhədlərdən kənara çıxır. Bununla əlaqədar yurisdiksiya ilə bağlı məsələnin aktuallığı artır. Bu məsələ ilə bağlı iki yanaşma mövcuddur [51].

Birinci yanaşma daha çox satıcılar üçün əlverişlidir və "mənşə ölkələri" və ya "satıcılar tərəfindən sərəncam verilir" prinsipinə əsaslanır. Belə bir ssenari üzrə elektron kommersiya ilə məşğul olan şirkətlər üstünlüyə malikdir. Çünki həmişə önü görünən və onlara yaxşı tanış olan hüquqi mühitdə fəaliyyət göstərirlər.

İkinci yanaşma, ilk növbədə, istehlakçıların maraqlarını qoruyur və "təyinat ölkələri" prinsiplərinə

əsaslanır. Burada şirkətlər üçün əsas problem müxtəlif hüquq sistemləri ilə toqquşmaq ehtimalıdır. Bu dillemmanın həllini nəzərdə tutan mexanizmlərdən biri istehlakçıların hüquqlarının müdafiəsi sahəsində müxtəlif ölkələrin qanunvericiliklərinin unifikasiyasıdır.

Avropa Birliyində istehlakçı hüquqlarının müdafiəsi yüksək səviyyədə təmin edilir. O cümlədən, yurisdiksiya problemi Avropa Birliyi ölkələrində məhkəmə qərarlarının yerinə yetirilməsi üzrə Brüssel Konvensiyası çərçivəsində həll edilir [36]. Konvensiyada tələb edilir ki, istehlakçıların öz hüquqlarının müdafiəsi üçün həmişə yerli hüquq-mühafizə orqanlarına və məhkəmələrə müraciət etmək imkanı yaradılsın.

Qlobal səviyyədə hər hansı beynəlxalq hüquqi vasitə yaradılmayıb. Ən əhəmiyyətli sənədlərdən biri olan Malların beynəlxalq alqı-satqı müqaviləsi haqqında BMT Konvensiyası (1980-ci il) istehlakçı müqavilələrinin bağlanması və istehlakçı hüquqlarının müdafiəsi məsələlərinə toxunmur [47].

Elektron kommersiyanın gələcək inkişafı bu sahədə istehlakçı hüquqlarının müdafiəsi üçün ya müxtəlif ölkələrin qanunvericiliklərinin unifikasiyasını, ya da yeni beynəlxalq rejimin yaradılmasını tələb edir.

ƏDƏBİYYAT

1. Наумов В.Б., Право и Интернет: Очерки теории и практики, М.: Книжный дом «Университет», 2002. 432 с.
2. www.isoc.org
3. www.icann.org
4. BCG и Colin Carter & Associates. Независимый анализ деятельности Совета директоров ICANN. Сводная информация и рекомендации, Ноябрь 2008 г., www.bcg.com
5. Kurbalija J., Gelbstein E. Internet Governance: Issues, Actors and Divides, DiploFoundation, 2005. – 183 p.
6. www.ec.europa.eu
7. www.nnm.ru
8. www.webplanet.ru
9. Рабочая группа по управлению Интернетом (информационная записка), www.ifap.ru
10. Доклад рабочей группы по управлению Интернетом, 2005., www.itu.int
11. www.un.org
12. www.internet-law.ru
13. Зенин И.А., Основы права / Московский международный институт эконометрики, информатики, финансов и права. - М.: 2003. - 184 с.
14. Серго А.С. Интернет и право, "Бестселлер", 2003. – 272 с.
15. www.upu.int

16. Малько А.В. Механизм правового регулирования: Лекция//Правове-дение. - 1996. - № 3 (214). - с. 54 – 62
17. Рассолов И.М. Право и Интернет. М., 2003. - 257 с.
18. Малова О.В. Правовой обычай, обыкновение и общепризнанные принципы и нормы международного права, Сибирский Юридический Вестник. - 2001. - № 4.
19. Бордунов В. Д., Международное воздушное право. Учебное пособие, М. : НОУВКШ "Авиабизнес"; изд-во "Научная книга", 2006. – 464 с.
20. Шлянцев Д.А. Международное право: курс лекций, М.: Юстицинформ, 2006. - 256 с.
21. www.zonazakona.ru
22. Под ред. Дмитриевой Г.К. Международное частное право. 2-е изд., перераб. и доп. - М.: ТК Велби, Проспект, 2004. — 688 с.
23. Ушаков Н.А. Международное право: Учебник. – М: Юрист, 2000. – 304 с.
24. Наумов В.Б. Проблема ответственности информационных провайдеров. Доклад на II Всероссийской конференции «Право и Интернет: теория и практика», www.ifap.ru
25. Шахов Н.И. Теоретико-правовые основы функции обеспечения госу-дарством права на неприкосновенность информации о частной жизни. Автореферат диссертация на соискание ученой степени кандидата

юридических наук, Краснодар – 2008.. www.jurisprudence-media.ru
26. www.america.gov
27. www.osce.org
28. Хосейн Г. Ограничение и сдерживание глобальных потоков данных. – М.: МЦБС, 2008. – 68 с.
29. Brain M., What is an IP address?, HowStuffWorks, www.com-puter.howstuffworks.com
30. www.echr.coe.int
31. www.portal.unesco.org
32. www.wikipedia.org
33. www.itu.int
34. www.wto.org
35. www.securelist.com
36. www.europa.eu
37. Бабкин С.А. Интеллектуальная собственность в Интернет. Изд-во: Центр ЮрИнфоР, 2006., 512 стр.
38. Судариков С.А. Основы авторского права., Мн.: Амалфея, 2000. - 512 с.
39. www.wipo.int
40. Зинина У.В. Защита прав интеллектуальной собственности в сети Интернет. www.ecsocman.edu.ru
41. Львовна Т.Т. Киберпреступность: понятие, состояние, уголовно-правовые методы борьбы. Автореферат диссертации на соискание ученой степени кандидата юридических наук, www.crime.vl.ru

42. Shinder D.L., Scene of the Cybercrime: Computer Forensics, Ed Tittel (Editor), 2002. - 29 p.
43. Дремлюга Р.И. Интернет-преступность, Монография. Владивосток: Изд-во Дальневост. Ун-та, 2008. – 240 с.
44. Калинина А.Е., Интернет-бизнес и электронная коммерция: Учебное пособие. - Волгоград, Изд-во ВолГУ, 2004. – 148 с.
45. Богдановская И.Ю. Правовое регулирование электронной коммерции: зарубежная практика, Доклад на II Всероссийской конференции «Право и Интернет: теория и практика», www.ifap.ru
46. Зажигалкин А.В. Международно-правовое регулирование электронной коммерции, Автореферат диссертации на соискание ученой степени кандидата юридических наук, www.russianlaw.net
47. www.uncitral.org
48. www.unctad.org
49. www.apec.org
50. Пластинина Н.В., Дистанционные покупки., Изд-во: Дашков и К, 2009. - 160 с.
51. Под ред. Попондопуло В.Ф. Международное торговое право., М.: Омега-Л, 2005. - 472 с.

Alguliev R.M, Mahmudov R.Sh. Problems of adjustment of Internet. Express-information. Series of Information Society
Baku: "Information Technologies" printed house, 2010, 115 p.

It investigates necessity and problems of the Internet regulation in research work. It also analyzes international initiatives and experience of leading countries in this field. The ways, legal mechanisms, and jurisdiction problems applied in adjustment are researched. Also other problems related to Internet - the problems of inviolability of private life and protection of the personal information, management of domain names' system, definition of legal responsibilities of providers, struggle against cybercrimes, spams, protection of intellectual property rights, and adjustment of activity of electronic commerce.

Алгулиев Р.М., Махмудов Р.Ш. Проблемы регулирования Интернета. Экспресс-информация. Серия «Информационное общество».
Баку: издательство «Информационные технологии», 2010, 115 с.

В исследовательской работе изучается необходимость и проблемы регулирования Интернета, анализируются международные инициативы, опыт ведущих стран в этой области. Исследуются способы, правовые механизмы и вопросы юрисдикции, применяемые при регулировании. А также изучается другие проблемы связанные с Интернетом - неприкосновенность личной жизни и защита личной информации, управление системой доменных имен, определение правовой ответственности провайдеров, борьба с киберпреступлениями, спамами, защита прав интеллектуальной собственности, регулирование деятельности электронной коммерции.

Əliquliyev
Rasim
Məhəmməd oğlu

AMEA İnformasiya Texnologiyaları İnstitutunun direktoru və "İnformasiya cəmiyyəti problemləri" şöbəsinin rəhbəri, AMEA-nın müxbir üzvü, texnika elmləri doktoru, professor

secretary@iit.ab.az
director@iit.ab.az

Mahmudov
Rasim
Şərif oğlu

AMEA İnformasiya Texnologiyaları İnstitutunun böyük elmi işçisi

depart17@iit.ab.az
rasim72@gmail.com

Texniki redaktor: Anar Səmidov

Korrektor: Ləman Manahova

Kompyuter dizaynı: Səlahət Hüseynova

Çapa imzalanmışdır 15.02.2010. Çap vərəqi 60x84.
Sifariş №24, sayı 100 ədəd