HÜQUQ

ORCHID ID: https://orcid.org/0000-0001-5305-7113

VİRTUAL MƏKAN, KİBERTƏHLÜKƏLƏR VƏ İNSAN HÜQUQLARININ MÜDAFİƏSİ

G.A.RZAYEVA
Bakı Dövlət Universiteti
gulnazaydin@yahoo.com

Müasir cəmiyyətdə dünyagörüşünün dəyişməsi və inkişafı eyni zamanda hüquqazidd davranışlara da öz təsirini göstərir. Ənənəvi üsulların dövrün tələblərinə cavab verdiyi bir şəraitdə insan hüquqlarına qəsd edən əməllərin törədilməsində yeni üsul və vasitə kimi İKT-dən daha çox istifadə olunur. Bu da kibercinayətlərlə mübarizənin gücləndirilməsini tələb edir. Məqalədə qlobal informasiya cəmiyyətində kibercinayətlərlə pozulan insan hüquqlarının müdafiəsi mexanizmlərinin işlənib hazırlanmasına dair təklif və tövsiyələr irəli sürülür.

Açar sözlər: qlobal informasiya cəmiyyəti, kiberməkan, kibercinayət, ifadə azadlığı, şəxsi toxunulmazlıq hüququ, əqli mülkiyyət hüququ, informasiya siyasəti.

Giriş

Qlobal informasiya cəmiyyətinin sürətlə inkişafı insan hüquqlarının müdafiəsi mexanizmlərinin, eləcə də onlara qarşı yönəlmiş pozuntularla mübarizənin də dünya miqyasında müzakirəsinə gətirib çıxarmışdır. Qlobal informasiya cəmiyyəti yeni tip cəmiyyətdir ki, burada informasiya dövriyyəsi zaman, məkan, siyasi sərhədlər tanımır və məhz biliklərin emalı nəticəsində cəmiyyətin həyatının bütün aspektlərdə yaxşılaşdırılması üçün əsaslı qərarlar verilə bilər. Bu cəmiyyətin əsas tələbi hər kəsin informasiya mübadiləsində iştirakının təmin edilməsi olduğu üçün hal-hazırda internet şəbəkəsi həyatımızın ayrılmaz hissəsinə çevrilmişdir. Təbii ki, İKT-nin imkanlarından məqsədyönlü istifadə ilə yanaşı, qeyri-qanuni əməllərin törədilməsi də qaçılmaz haldır. Hətta, ənənəvi cəmiyyətdə mövcud olan cinayətlərin də kiberməkanda yeni törədilmə üsulları formalaşmışdır ki, bu da "kibertəhlükə" problemini gündəmə gətirmişdir. İnformasiya cəmiyyətinin ilikin dövrlərində kiberməkanda törədilən pozuntular yalnız informasiya hüquqlarına qəsd edirdisə, artıq bu gün İKT-dən istifadə etməklə törədilən cinayətlər müxtəlif insan hüquqlarını pozur. Bu da kibertəhlükələrə qarşı mübarizənin həm beynəlxalq, həm də milli səviyyədə gücləndirilməsini zəruri edir.

1.1. Kibermәkan, yoxsa virtual mәkan?

İnformasiya cəmiyyətinin qloballaşması ***"kibermәkan"***[1] termininin yaranmasına gətirib çıxarmışdır. "Kibermәkan" anlayışı ilk dəfə 1982-ci ildə Uilyam Qibson tərəfindən "Yanan xrom" (Burning Chrome) [7], az sonra isə 1984-cü ildə "Neuromancer" [8] əsərində istifadə edilmişdir.

ABŞ Ali Məhkəməsinin verdiyi anlayışa görə: "Kibermәkan konkret ərazisi olmayan, lakin dünyanın istənilən nöqtəsində internet vasitəsilə hər kəs üçün açıq və əlyetər olan unikal daşıyıcıdır." Darrel Ment "internasional məkanlar nəzəriyyəsi"ni şərh edərək, üç belə məkan olduğunu yazır: Antarktika, kosmos və açıq dəniz. Müəllif dördüncü belə məkan qismində kibermәkan olduğunu qeyd edir və bu məkana dövlət suverenliyinin şamil olunmadığını vurğulayır [3, p.70]. Maraqlı cəhət ondadır ki, kibermәkanda yurisdiksiya məsələlərini araşdıran tədqiqatçı yalnız müəlliflik hüququ və böhtanla bağlı tərəfləri izah edir. Bu zaman belə bir sual ortaya çıxır: Əgər kibermәkana heç bir dövlətin suverenliyi şamil olunmursa, onda bir dövlətin qanunvericiliyinin hər hansı bir məlumatın internetə yerləşdirilməsini qadağan etməsi nə dərəcədə qanunauyğun hesab oluna bilər? Və yaxud dövlət öz vətəndaşlarının istənilən informasiyaya çıxışını məhdudlaşdıra bilərmi? – Bütün bu kimi sualların cavablandırılması üçün kibermәkanın əsaslandığı prinsiplər normativ təminata malik olmalıdır. Təsadüfi deyil ki, 22 iyul 2000-ci il tarixdə "Böyük Səkkizlik"[2] dövlətləri tərəfindən qəbul edilmiş "Qlobal İnformasiya Cəmiyyətinin Okinava Xartiyası"nda dövlətlər siyasi, normativ və şəbəkə təminatını İKT-nin sonrakı inkişafı üçün zəruri tədbirlər sırasında qeyd etmişlər.

Müasir dövrdə kibermәkanın müstəqilliyinə dair çıxışlar səsləndirilir. Məsələn, 1996-cı ildə Davos forumunda Elektron Sərhəd Fondunun yaradıcısı Con Perri Barlou özünün məşhur "Kibermәkanın müstəqilliyi" adlı Bəyannaməsini elan etdi. Bəyannamədə bütün dövlətlərə belə bir müraciət ünvanlanır: "Kibermәkan sizin sərhədlərinizə aid deyil. Elə düşünməyin ki, onu siz yaratmısınız. Kibermәkan ictimai layihədir. Bizim aramızda sizə yer yoxdur. Siz kibermәkanda üstün hakimiyyətə malik deyilsiniz. Bizim üzərimizdə hökmranlıq etməyə sizin nə mənəvi haqqınız, nə də məcburetmə metodlarınız var. Biz kibermәkanda sizin qurduğunuzdan daha ədalətli və humanist olan cəmiyyət yaradacağıq…" [21] Belə çıxışların səslənməsinə baxmayaraq, kibermәkanla bağlı məsələlər hələ də hər bir dövlətin öz yurisdiksiyası çərçivəsində həll olunur. Təbii ki, bu zaman beynəlxalq hüquq normaları və prinsipləri nəzərə alınır.

"Kibermәkan" anlayışının təhlili məqsədilə "informasiya məkanı", "İnternet" və s. bu kimi terminlərin məzmununa aydınlıq gətirilməsi, onların arasında fərqin müəyyən edilməsi məqsədəmüvafiqdir. İnternet – informasiyanın

[1] "Kiber" – "kibernetika" sözündən yaranmışdır. "Kibernetika" termini qədim yunan dilində "kibernetes" sözündən götürülmüş, "idarə edən" mənasını verir.

[2] Almaniya, ABŞ, Böyük Britaniya, Fransa, Yaponiya, Kanada, Rusiya, İtaliya.

saxlanması və ötürülməsi üçün yaradılmış kompüter şəbəkələrinin ümumdünya sistemidir. Ona görə də əksər hallarda İnternet "qlobal şəbəkə", "ümümdünya şəbəkəsi" kimi adlandırılır. Bu şəbəkəni kiberməkanla eyniləşdirmək olmaz. Darrel Ment yazır ki, biz İnternetin haradan başlandığını bilirik, amma kiberməkanın sərhədlərini və məhz hardan başlandığını müəyyənləşdirmək qeyri-mümkündür. Ona görə də kiberməkan anlayışı İnternetlə eyniləşdirilə bilməz [3, p. 69-70]. Tədqiqatçının mövqeyini məqbul saymaq olar, yəni kompüter şəbəkələrinin vahid sistemi olan İnternetdən fərqli olaraq, kiberməkan metaforik abstrakt, virtual reallıq kimi qiymətləndirilməlidir. Qısa sözlə desək, kiberməkan ümumdünya kompüter şəbəkəsinin içində sərhədləri bilinməyən bir "aləmdir". Ona görə də əksər hallarda bu aləmi xarakterizə etmək üçün ***"virtual məkan"*** anlayışından istifadə edilir. Məsələ burasındadır ki, beynəlxalq normalarda hüquqi termin olaraq, "kiberməkan" anlayışına müraciət olunur. Lakin milli hüquqda isə "virtual" terminə bir çox normativ aktlarda rast gəlmək olar. Həmin normativ aktların məzmununa əsasən, deyə bilərik ki, dövlətdaxili hüquqda "virtual" adı altında İnternet vasitəsilə qurulan münasibətlər başa düşülür. Hətta, Virtual Azərbaycan [18], Virtual Qarabağ [20] və s. bu kimi saytlar yaradılmış və fəaliyyət göstərir. Hətta, "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair Milli Strategiyanın həyata keçirilməsi üzrə 2016-2020-ci illər üçün Dövlət Proqramı"nda "Azərbaycan həqiqətlərinin virtual məkanda təbliği və yayılmasının genişləndirilməsi üzrə tədbirlər görülməsi" milli kontentin inkişaf etdirilməsi üzrə tədbirlər sırasında qeyd olunmuşdur. Eyni zamanda, azərbaycandilli mənbələrdə "virtual cəmiyyət" "İnternet cəmiyyət"lə eyniləşdirilərək, elektron fəzada yaranan və fəaliyyət göstərən yeni tip cəmiyyət kimi şərh olunur.

Ədəbiyyatda hər iki terminlə bağlı yanaşmalardan açıq-aydın görünür ki, məna baxımından həm kiberməkan, həm də virtual məkan kompüter şəbəkəsindən istifadə edilməklə qurulan və gözlə görülə bilməyən bir aləmdir. İngilisdilli ədəbiyyatlarda kiberməkan anlayışına daha çox rast gəlinir. Lakin bununla belə, "virtual mühit", "virtual aləm" [19], "virtual dünya" [11] kimi anlayışlardan da istifadə edilir və verilən anlayışlardan bunların hamısının kiberməkanla eyni məzmuna malik olması nəticəsinə gələ bilərik. Lakin fərqli şərhlər də vardır. Belə ki, bəzi tədqiqatçılar kiberməkan və virtual reallığın hər ikisinin İnternet şəbəkəsi, KİV-lə bağlı olduğunu qeyd edərək yazırlar: "Hipermediya iki funksiya icra edə bilər: obyektiv aləmdə pəncərə funksiyası və subyektiv aləmin güzgüsü funksiyası. Birinci funksiya virtual reallığı, ikinci isə kiberməkanı əhatə edir. Yəni virtual reallıq dəqiq qavranılan aləmi əks etdirirsə, kiberməkan həmin aləmin dəqiq konseptual əsasını müəyyən edir." [13] Rusdilli ədəbiyyatlarda isə "virtual məkan" ya "cyberspace" kateqoriyasının tərcüməsi kimi qiymətləndirilir [16, с. 742], ya da bu anlayışların sinonim olduğu iddia edilir [15, с. 6]. Fikrimizcə, "kiberməkan" və "virtual məkan" hər ikisi abstrakt və sinonim anlayışlardır. Sadəcə olaraq, nəzəri yanaşmadan asılı olaraq bəzi müəlliflər birinci, bəzi müəlliflər isə ikinci ter-

mindən istifadə edirlər. Yəni daha çox texniki və idarəetmə aspektindən yanaşdıqda, kiberməkan, sosial-humanitar movqedən yanaşdıqda isə virtual məkan anlayışına müraciət olunur. Nəzərə alsaq ki, hal-hazırda dünyada internetdən başqa, alternativ şəbəkə yoxdur, virtual məkan və kiberməkan anlayışları sırf internet müstəvisində şərh olunmalıdır.

1.2. Kibertəhlükələrlə pozulan insan hüquqlarının müdafiəsi

Müasir cəmiyyətdə məlumatların yayılması, ötürülməsində başlıca vasitəyə çevrilmiş kiberməkanda şəxsi toxunulmazlıq hüquqlarının pozulmasına və şəxsi həyata dair məlumatların qeyri-qanuni üsullarla və qeyri-qanuni məqsədlər üçün istifadəsinə də az rast gəlinmir. Ona görə də bu problemin həlli dünya ictimaiyyətinin qarşısında dayanan vacib məsələlərdən biridir.

Kiberməkanda şəxsi toxunulmazlığın qorunması problemi hələ XIX əsrin sonlarından ABŞ-da irəli sürülməyə başlanmışdı. Belə ki, 1890-cı ildə Harvard Hüquq İcmalında dərc olunan Samuel Uorren (1852-1910) və Luis Brendaysın (1856-1941) dərc etdirdiyi "Şəxsi həyatın toxunulmazlığı" adlı məqalədə şəxsi həyata dair bir çox vacib məqamlar öz əksini tapmışdır. Məqalədə deyilir: "Şəxsi həyatın və mülkiyyətin toxunulmazlığı əslində əvvəlki dövrlərdən ümumi hüquqda tanınmışdır. Belə ki, əvvəllər qanun (hüquq) daha çox fiziki müdaxilələrin qarşısının alınması vasitələrini nəzərdə tuturdu və "vi et armis" (silahın gücü ilə) prinsipi rəhbər tutulurdu. Lakin tədricən baş verən sosial, siyasi və iqtisadi dəyişikliklər insanın intellektinin ön plana çəkilməsinə və nəticə etibarilə, şəxsi həyatın və mülkiyyətin toxunulmazlığı kimi hüquqların əhatə dairəsinin genişlənməsinə gətirib çıxardı. Bununla da, şəxsi toxunulmazlıq hüququ bir sıra imtiyazları ehtiva etməyə başladı və artıq mülkiyyət toxunulmazlığı yalnız maddi deyil, həmçinin qeyri-maddi formada sahibliyi əhatə etdi..." [12, p. 193-220]

Deməli, artıq əvvəllər olduğu kimi, şəxsi həyatın toxunulmazlığı məsələsi hər hansı bədən xəsarətləri ilə bağlı meydana gəlmirdi və intellekt, informasiya özü şəxsi həyatın toxunulmazlığında əsas element kimi qiymətləndirilirdi. Bununla yanaşı, şəxsi toxunulmazlığın insanın fiziki bədənindən asılı olmayaraq müəyyənləşdirilməsi insanın ailə münasibətlərini şəxsi həyatın toxunulmazlığı konsepsiyasının bir hissəsinə çevirdi. S.Uorren və L.Brendaysın öz məqaləsini yazmaqda əsas məqsədi məhz belə bir yeni şəraitdə şəxsi həyatın toxunulmazlığı, təhqir, böhtan və s. bu kimi məsələlərin qanunla necə tənzimlənməsini və təcrübi tərəfləri təhlil etməkdən ibarət idi. Məqalənin maraqlı tərəfi ondadır ki, müəlliflər bir çox Roma hüququnun prinsiplərinə (postulatlarına) müraciət edirlər. Məsələn, "damnum absque injuria"[1] prinsipini rəhbər tutan tədqiqatçılar xüsusi vurğulayırlar ki, hətta formal olaraq qanuni və leqal görünən hər hansı bir hərəkət insanın şəxsi həyatına qəsd edə bilər.

[1] **Damnum absque injuria** – latın dilindən götürülüb, delikt hüququnun prinsiplərindən biridir və şəxsə fiziki zərər yetirmədən hər hansı bir itkiyə məruz qoymanı ifadə edir.

Müəlliflər Prins Albert v. Strencin və Vilsonun məhkəmə işlərini misal göstərərək, Lord Kottenhamın "III Georginin xəstəliyi zamanı onun ətrafında olmuş həkimlərin öz gündəliklərindəki qeydləri çap etməyin düzgün olmadığı" iddiasını xüsusi qeyd edirlər [4].

S.Uorren və L.Brendays öz məqaləsində həmçinin şəxsi toxunulmazlıq hüququnun Fransa qanunvericiliyində əks olunan tərəflərinə də nəzər salırlar: şəxsi toxunulmazlıq hüququ dövlət və ictimai maraq kəsb edən hər hansı bir məsələ üzrə nəşri qadağan etmir; şəxsi toxunulmazlıq hüququ müxtəlif formalarda kommunikasiyanı (rabitəni) qadağan etmir; şəxsi toxunulmazlıq hüququ faktın dərc olunmasına icazə verildiyi və ya onun dərc olunduğu andan başa çatmış hesab olunur və s.

Şəxsi həyatın toxunulmazlığı problemi sonralar Uilyam Lloyd Prosserin (1898-1972) 1960-cı ildə dərc etdirdiyi məqaləsində daha geniş təhlil olunmuşdur. Belə ki, müəllif şəxsi həyatın toxunulmazlığının pozulması ilə müşayiət olunan dörd növ delikti fərqləndirirdi:

1. Şəxsin həyatına və mənzilinə irrasional müdaxilə;
2. Şəxsi məlumatların açıqlanması;
3. Şəxs haqqında məlumatların təhrif olunması, yəni yalan məlumatların yayılması;
4. Şəxsin adı, soyadı və portretinin gəlir əldə etmək məqsədilə qanunsuz əldə olunması və ya istifadəsi [14, p. 389].

Göründüyü kimi, ilkin olaraq, gənc tədqiqatçılar tərəfindən irəli sürülmüş şəxsi həyatın toxunulmazlığı hüququ müasir dünyada fundamental insan hüquqlarından biri kimi həm beynəlxalq səviyyədə, həm də ayrı-ayrı dövlətlərin milli hüququnda tanınmışdır.

Hal-hazırda Azərbaycan Respublikasında fərdi məlumatların qorunması sahəsində həm hüquqi istiqamətdə, həm də təcrübi baxımdan böyük uğur əldə olunmuşdur. Hüquqi baza barəsində fərdi məlumatların təhlili zamanı yetərincə məlumat verilmişdir. O ki qaldı təcrübi tərəflərə, ölkə daxilində elektronlaşdırma proseslərinin sürətlə həyata keçirilməsi, elektron imzanın tətbiqi və digər müxtəlif kriptoqrafik üsullardan istifadə hal-hazırda şəxsi həyatın toxunulmazlığı hüququna müdaxilələrin sayını xeyli aşağı salmışdır.

Şəxsi toxunulmazlıq hüququndan fərqli olaraq, əqli mülkiyyət hüquqlarının virtual məkanda müdafiəsində çoxsaylı ziddiyyətlər mövcuddur. Azərbaycan Respublikası Müəllif Hüquqları Agentliyinin sədri K.S.İmanov kibermə-kanda əqli mülkiyyət hüquqları problemini iki istiqamətdə şərh edir. Müəllifin yanaşmasına görə, birincinin mahiyyəti ondan ibarətdir ki, hüquq sahibləri intellektual məhsulun yaradılması və yayılmasından tam gəlir əldə edə bilmirlər. Çünki rəqəmsal dövrdə istifadəçilər üçün məlumatın, yəni rəqəmsal məzmunun surətini çıxarmaq ucuz başa gəlir və onlar uzaq məsafələrdə və böyük həcmdə məlumatların mübadiləsini aparmaq imkanına malikdirlər. Bu halda nüsxələrin mükəmməl dəqiqliklə və sıfır həddində olan məsrəflə çoxaldılması və onların ani sürətdə və yenə də sıfır məsrəflə yayılması üçün görünməmiş

imkanlar var. İkinci münaqişə isə ondan ibarətdir ki, hüquq sahibləri çox vaxt faktiki hüquq pozucuları olan istifadəçilərə qarşı onların anonimliyi və qeyri-leqal məzmun mübadiləsinin geniş yayılması səbəbindən iddia irəli sürə bilmirlər və buna görə də günahı provayderlərin üzərinə qoyurlar [1, s. 386].

Kiberməkanda əqli mülkiyyət hüquqlarının qorunması ilə bağlı ən başlıca problem ondan irəli gəlir ki, İnternetin açıqlığı, yəni məlumatların asan əldə edilməsi əqli mülkiyyət hüquqlarının pozulması hallarını daha da artırır. Hətta, müəlliflər bu cür ziddiyyəti "İnternet – Copyright" konflikti kimi adlandırırlar [6, p. 197-213].

İnternetdə əqli mülkiyyət hüquqlarının qorunmasına dair iki yanaşma mövcuddur. Birinci yanaşmaya görə, İnternetdə əqli mülkiyyət hüquqlarının qorunmasına ehtiyac yoxdur, bu İnternetin inkişafına mane ola bilər. Ən yaxşı halda şəxsin qeyri-əmlak hüquqlarının tanınması kifayət edir. İkinci yanaşma isə əksinə, İnternetdə əqli mülkiyyət hüquqlarının qorunmasını zəruri sayır, bu məqsədlə "hüquqların kollektiv idarə edilməsi" üsulunu təklif edir. Bu üsul o vaxt tətbiq edilir ki, müəlliflik və əlaqəli hüquqların fərdi qaydada müdafiəsi çətin olur. Belə halda əqli mülkiyyətin obyektlərindən istifadə olunur, əvəzində hüquq sahiblərinə müəyyən olunmuş qaydada haqq ödənilir [5, p. 238-252].

Kiberməkanda əqli mülkiyyət hüquqlarının qorunması ilə bağlı YUNESKO-nun fəaliyyəti xüsusi qeyd olunmalıdır. 2006-cı ilin yanvarında təşkilat "Rəqəmsal əsrdə hüquq və cəmiyyət" tədqiqat layihəsinə start verdi. Layihənin əsas məqsədi əqli mülkiyyət sahibləri və istifadəçilər arasında kompromisin əldə olunması idi. İlkin fəaliyyət rəqəmsal formada ifadə olunan əqli mülkiyyət obyektlərinə dair hüquqlarla bağlı sorğunun keçirilməsi ilə başlandı. Sorğunun nəticələrinə əsasən, bir çox maraqlı faktlar üzə çıxarıldı. Məsələn, sorğuda iştirak edən hüquq sahiblərinin 51%-i hesab edirdi ki, piratçılığın artmasında əsas səbəb qismində yalnız qanunvericilikdəki boşluqlar deyil, həmçinin istehlakçıların hüquq düşüncəsinin aşağı səviyyədə olması çıxış edir. Həmçinin başqa bir misal: İstifadəçilərin 46%-i və hüquq sahiblərinin 44%-i qeyri-kommersiya məqsədləri üçün pirat məhsulların yayılmasının ümumiyyətlə cəzaya məruz qalmamasının tərəfdarı kimi çıxış edirdilər. Əksinə kommersiya məqsədilə pirat məhsul istehsalına görə daha sərt cəzalar müəyyən olunmasını zəruri sayırdılar [17, c. 9-12].[1]

Kiberməkan informasiyanın dövr etdiyi bir məkan olduğu üçün burada ifadə azadlığından sui-istifadə halları da insan hüquq və azadlıqlarına qəsd edir. Belə ki, sırf ifadə azadlığının realizə olunması ilə törədilən cinayətləri şərti olaraq iki qrupda ayırmaq olar:

[1] Туликов А. Интеллектуальная собственность в киберпространстве: правообладатели и общество готовы к диалогу. // Интеллектуальная собственность в киберпространстве: Сборник аналитических материалов проекта "Право и общество в цифровую эпоху". МОО ВПП ЮНЕСКО "Информация для всех". Составитель: Евгений Альтовский, 2006, с. 9-12.

1. Kiberməkandan cinayətin törədilməsi vasitəsi kimi istifadə olunan, müxtəlif obyektə – ictimai münasibətlərə qəsd edən cinayətlər. Məsələn, təcavüzkar müharibəni başlamağa açıq çağırışlar (Cinayət Məcəlləsinin 101-ci maddəsi) sülh və insanlıq əleyhinə cinayətlərə, milli, irqi, sosial və ya dini nifrət və düşmənçiliyin salınması isə (Cinayət Məcəlləsinin 283-cü maddəsi) dövlətin konstitusiya quruluşunun əsasları və təhlükəsizliyi əleyhinə olan cinayətlərə daxildir. Lakin hər iki cinayətin törədilməsində kütləvi informasiya vasitələrindən istifadə olunarsa, daha ağır cəza tətbiq edilir. Təbii ki, kiberməkandan istifadə edilməklə, bu cinayətlərin törədilməsi ifadə azadlığının qeyri-qanuni formada realizəsi deməkdir.

2. Hər bir halda kiberməkandan istifadə edilməklə törədilən şərəf və ləyaqətə qəsd edən cinayətlər. Bu cinayətlər fikir və söz azadlığının həm şifahi, həm də yazılı formada həyata keçirilməsi zamanı icra edilə bilər. Məsələn, təhqir (Azərbaycan Respublikası Cinayət Məcəlləsinin 148-ci maddəsi), böhtan (Azərbaycan Respublikası Cinayət Məcəlləsinin 147-ci maddəsi) və Azərbaycan dövlətinin başçısının - Azərbaycan Respublikası Prezidentinin şərəf və ləyaqətini ləkələmə və ya alçaltma (Azərbaycan Respublikası Cinayət Məcəlləsinin 323-cü maddəsi) cinayətləri.

İfadə azadlığından kiberməkanda sui-istifadə halları son illərdə ***nifrət nitqi*** ilə bağlı məsələləri gündəmə gətirmişdir. Avropa Şurasının Nazirlər Komitəsinin Tövsiyəsinin 97(20) verdiyi anlayışa görə: "Nifrət nitqi dedikdə, irqi nifrət, ksenofobiya, anti-semitizm və ya aqressiv millətçilik və etnosentrizmlə ifadə olunan dözümsüzlük, azlıqlara, miqrantlara və immiqrant mənşəli şəxslərə ayrı-seçkilik və düşmənçilik də daxil olmaqla, dözümsüzlüyə əsaslanan nifrətin digər formalarını yayan, təhrik edən, təşviq edən və ya əsaslandıran ifadənin bütün formaları başa düşülür." [10]

Son dövrlərdə fikir və söz azadlığının normal şərtlər altında həyata keçirilməsi məqsədilə həm beynəlxalq, həm də milli səviyyədə bir sıra tədbirlər icra olunur. Belə ki, 47 ölkəni birləşdirən Avropa Şurası tərəfindən Gənclər Sektorunda 2012-2017-cü illər üzrə prioritet təşəbbüs kimi *"No Hate Speech Movement" – "Nifrət Nitqinə Yox Hərəkatı"* kampaniyası reallaşdırılmağa başlanmışdır. Bu kampaniya bərabərliyi, ləyaqəti, insan hüquqlarını, müxtəlifliyi müdafiə edir və dəstəkləyir. Kampaniyanın məqsədi gəncləri və gənclər təşkilatlarını bu cür insan haqları pozuntularını üzə çıxarmaq və belə hallara qarşı çıxış etmək üçün zəruri bacarıqlarla təmin etməklə, irqçilik və ayrıseçkilik məzmunlu nifrət nitqinin onlayn ifadəsinə qarşı mübarizə aparmaqdır.

Azərbaycanı Avropa Gənclər Forumunda tam hüquqlu üzv olaraq təmsil edən, Avropa Şurasının Gənclər üzrə Məşvərət Şurasının üzvü seçilmiş Azərbaycan Respublikası Gənclər Təşkilatları Milli Şurası bu kampaniyanın Azərbaycan üzrə milli əlaqələndiricisi olaraq, 2013-cü ilin may ayından etibarən "Nifrət Nitqinə Yox Hərəkatı"-na qoşulmuş və bu çərçivədə bir sıra tədbirlər həyata keçirmişdir. Bunlar sırasına Beynəlxalq Gənclər Gününə həsr edilən Gənclər Həftəsi, "Nifrət Nitqinə Yox Hərəkatı" fotosərgisi, Qəbələ rayonunda "Nifrət Nitqinə Yox Hərəkatı" Beynəlxalq Gənclər Forumu, "Nifrət Nitqinə Yox

Hərəkatı" adlı beynəlxalq forumu, "Qərbdən - Şərqə Nifrət Nitqinə Yox" regional forumu və bir sıra müxtəlif tədbirlər aiddir.

1.3. Kibertəhlükələrin qarşısının alınması üzrə tədbirlər

Kibertəhlükələrin qarşısının alınması üzrə tədbirləri şərti olaraq ümumi və xüsusi tədbirlərə bölmək olar. Xüsusi tədbirlərə insanların özünün həmin təhlükələrdən qorunması üzrə aktivlik dərəcəsini daxil etmək olar. Bu mənada, informasiya təhlükəsizliyi mədəniyyətinin mövcudluğu xüsusi əhəmiyyətə malikdir.

İnformasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması istiqamətində əsas mənbə - BMT Baş Məclisinin 20 dekabr 2002-ci il tarixli 57/239 saylı qətnaməsi ilə təsdiq edilmiş ***"Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması"*** və ona əlavə olan ***"Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər"***dir. "Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər"ə görə, iştirakçılar informasiya sistemlərinin və şəbəkələrin təhlükəsizliyinin zəruriliyi haqqında və təhlükəsizliyin yüksəldilməsi üçün onların nə edə biləcəkləri barədə məlumatlı olmalıdırlar, eləcə də onlar informasiya sistemlərinin və şəbəkələrin təhlükəsizliyi üçün öz rollarına uyğun olaraq cavabdehlik daşıyırlar. İştirakçılar təhlükəsizliyə aid insidentlərin qarşısının alınması, onların aşkarlanması və onlara cavab verilməsi üzrə vaxtında və birgə tədbirlər görməlidirlər. Onlar lazımi hallarda təhdidlər və boşluq faktorları haqqında məlumat mübadiləsi etməli və belə insidentlərin qarşısının alınması, onların aşkarlanması və onlara cavab verilməsi işində operativ və səmərəli əməkdaşlığı nəzərdə tutan prosedurlar tətbiq etməlidirlər. Bu transsərhəd informasiya mübadiləsini və əməkdaşlığı nəzərdə tuta bilər. Təhlükəsizlik elə təmin edilməlidir ki, bu fikir və ideyaların mübadiləsinin sərbəstliyi, azad informasiya axını, informasiya və kommunikasiyanın konfidensiallığı, şəxsi xarakterli informasiyanın lazımi şəkildə qorunması, açıqlıq və aşkarlıq daxil olmaqla demokratik cəmiyyətdə qəbul edilən dəyərlərə uyğun olsun [2].

Göründüyü kimi, "Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması üçün elementlər" yalnız istifadəçilər üçün deyil, konkret dövlətlər üçün bir sıra vəzifələr müəyyənləşdirir. Bu da informasiya təhlükəsizliyi mədəniyyətinin dövlətin marağında olan problem olmasını bir daha təsdiq edir. Məhz ona görə də Azərbaycan Respublikası Prezidentinin 6 dekabr 2016-cı il tarixli Fərmanı ilə təsdiq edilmiş "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi"ndə informasiya təhlükəsizliyi üzrə ümummilli hazırlıq və maarifləndirmə səviyyəsinin artırılması strateji məqsədlər sırasında əks olunmuşdur. Milli strategiyalarda isə informasiya təhlükəsizliyi mədəniyyətinin yüksəldilməsi belə maarifləndirmə işi üzrə gözlənilən nəticələrdən biri kimi nəzərdə tutulmuşdur.

Kibertəhlükələrin qarşısının alınması üzrə ümumi tədbirlər isə dövlət tərəfindən həyata keçirilir. Birinci növbədə, müxtəlif pozuntulara görə məsu-

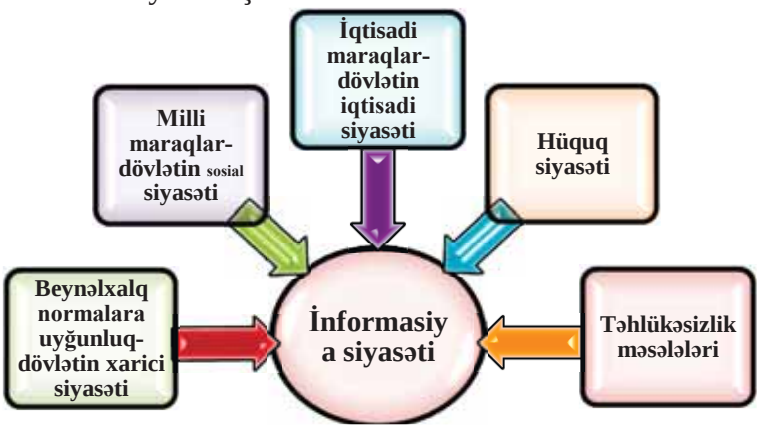
liyyətin müəyyən olunması və sanksiyaların təyin edilməsi qeyd olunmalıdır. Ənənəvi olaraq, hüquq pozuntularının xarakterindən asılı olaraq dörd növ – cinayət, inzibati, mülki və intizam məsuliyyəti fərqləndirilir. Lakin müasir dövrdə beynəlxalq-hüquqi məsuliyyət, konstitusiya-hüquqi məsuliyyət kimi anlayışlara da rast gəlinir. Bəs informasiya hüquqi məsuliyyət hansı növə aiddir və necə tənzimlənir? – Məsələ burasındadır ki, informasiya sahəsində münasibətlərin realizəsi zamanı törədilən hüquq pozuntularına görə sanksiyalar informasiya qanunvericilik aktlarında təsbit olunmamışdır. İctimai təhlükəli olan informasiya-hüquq pozuntuları cinayət qanunvericiliyində, inzibati xətanın əlamətləri ilə səciyyələnən pozuntular inzibati qanunvericilikdə, müxtəlif deliktlər mülki qanunvericilikdə nəzərdə tutulmuşdur və s. Belə olan halda, informasiya-hüquqi məsuliyyətin ayrıca bir institut kimi fərqləndirilməsinə ehtiyac varmı? – Leqal aspektdən yanaşsaq, xeyr. Lakin informasiya sahəsinin sərhədsiz olmasını, informasiya-hüquq pozuntuları ilə bağlı problemlərin və kolliziyaların mövcudluğunu nəzərə alsaq, həmin problemlərin cinayət, mülki və inzibati hüquq sahələri üzrə şərhi mümkün deyil. Məsələn, kibertəhlükələr, informasiya təhdidləri nəinki konkret vətəndaşa qarşı yönəlir, hətta böyük bir xalqın mənəviyyatına mənfi təsir göstərir. Belə təhlükələrin qarşısının alınması üzrə təklif və tövsiyələrin işlənməsi isə yalnız informasiya hüquq elmi çərçivəsində mümkün ola bilər. Bütün bunları rəhbər tutaraq, informasiya-hüquqi məsuliyyətin müstəqil bir hüquqi institut kimi təhlilini məqsədyönlü hesab edirik.

Digər bir ümumi tədbirlər planı milli informasiya siyasətinin istiqamətləri sırasında informasiya təhlükəsizliyinin təminatı qeyd olunmalıdır. YUNESKO-nun İnformasiya hamı üçün (İnformation for All) Proqramı Milli İnformasiya Cəmiyyəti Siyasətində (MİCS) beş prioritet müəyyənləşdirir: İnformasiya inkişaf üçün; İnformasiya mədəniyyəti; İnformasiyanın saxlanması; İnformasiya etikası; İnformasiya əlyetərliyi [9, p. 9-10].

Göründüyü kimi, milli informasiya siyasəti bütövlükdə cəmiyyət üçün informasiyanın əlyetərliyinin təminatına yönəlmiş tədbirlər və qaydalar sistemini özündə birləşdirir. Həll onunan məsələlərin xarakterindən asılı olaraq informasiya siyasəti 2 yerə bölünür: ***informasiya strategiyası*** **və** ***informasiya taktikası. İnformasiya strategiyası*** böyükhəcmli informasiya problemlərinin həllinə yönəlmiş planlı fəaliyyət modelidir ki, bu model nəticə etibarilə informasiyalaşdırma proseslərinin uğurla başa çatmasına və informasiya hüquq və azadlıqlarının maneəsiz təminatına yönəlmişdir. ***İnformasiya taktikası*** isə informasiya strategiyasının əsasında formalaşır, qarşıya qoyulan məqsəd və vəzifələrə çatmaq üçün icra olunan konkret tədbirləri əhatə edir. Bu o deməkdir ki, informasiya strategiyası "nə" və "niyə" suallarını cavablandırırsa, informasiya taktikası "necə" sualına cavab verir. Strategiyadan fərqli olaraq, informasiya taktikası çevikliyi ilə xarakterizə olunur. Məsələn, Azərbaycan Respublikası Prezidentinin 17 fevral 2003-cü il tarixli 1146 nömrəli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının inkişafı naminə informasiya və

kommunikasiya texnologiyaları üzrə Milli Strategiya (2003-2012-ci illər)”nın icrası məqsədilə bir sıra dövlət proqramları – “Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan)” və s. qəbul edilmişdir ki, bu proqramlar dövlətin informasiya taktikasını əks etdirir.

Milli informasiya siyasətinin həyata keçirilməsi dövlətin fəaliyyətinin digər aspektləri nəzərə alınmadan qeyri-mümkündür. Belə ki, iqtisadi baxımdan səmərəsiz bir şəraitdə informasiyalaşdırma və elektronlaşdırma proseslərindən, informasiya əlyetərliyinin təminatından danışmaq bir qədər məntiqsiz olar. Digər tərəfdən milli maraqları nəzərə almayan informasiya siyasəti uğurla icra oluna bilməz. Həmçinin beynəlxalq normalara riayət etmədən həyata keçirilən və hüquqi bazası olmayan informasiya siyasəti nəticədə maraqların toqquşmasına gətirib çıxaracaqdır. Başqa bir tərəf onda özünü büruzə verir ki, milli təhlükəsizlik qorunmadığı bir şəraitdə informasiya siyasətinin normal icrasına nail olmaq mümkünsüzdür. Təsadüfi deyil ki, “Milli təhlükəsizlik haqqında” 29 iyun 2004-cü il tarixli Azərbaycan Respublikası Qanununda informasiya sahəsində milli təhlükəsizliyin təmin olunması ayrıca bir sahə kimi nəzərdə tutulmuşdur: “Azərbaycan Respublikasının milli təhlükəsizliyi siyasi, iqtisadi, hərbi, sosial, informasiya, ekologiya, elm, mədəniyyət, mənəviyyat və digər sahələr üzrə təmin olunur” (maddə 15.1). Ona görə də dövlətin informasiya siyasəti beynəlxalq və milli maraqlar nəzərə alınmaqla, milli təhlükəsizlik təmin olunmaqla, iqtisadi və hüquqi tədbirlərlə qarşılıqlı əlaqəli formada həyata keçirilir:



Yuxarıdakı sxemdən açıq-aydın görünür ki, milli informasiya siyasəti dedikdə, dövlət orqanları tərəfindən həyata keçirilən kompleks tədbirlər sistemi başa düşülür. Belə bir sual ortaya çıxır: Milli informasiya siyasətinin yalnız dövlət hakimiyyət orqanlarında çəmləşməsi insan hüquq və azadlıqlarının məhdudlaşdırılması anlamına gətirə bilərmi? – Xeyr. Əslində, hüquq və azadlıqların təminatı, hüquq pozuntularının qarşısının alınması və s. bu kimi vəzifələrin icrası üçün dövlət hər bir zaman idarəedici təsisat olaraq mövcud

olmuşdur. Hüquqi dövlət ideyasının geniş vüsət aldığı bir dövrdə dövlətin rolu olmadan qarşıya qoyulan məqsədlərə nail olmaq mümkün deyil. Təbii ki, dövlət orqanlarının özünün də fəaliyyətinə nəzarət olunması vacib faktorlardan sayılır. Məhz ona görə də hüquqi dövlətin əsas prinsiplərindən biri kimi "qarşılıqlı məsuliyyət, yəni şəxsin dövlət qarşısında və dövlətin şəxs qarşısında məsuliyyəti" hər zaman rəhbər tutulur. Bununla yanaşı, açıq hökumət, ictimai nəzarət, vətəndaş cəmiyyəti və digər ideyaların ön plana çəkilməsi dövlətin milli informasiya siyasətinin həyata keçirilməsinə mühüm təsirini göstərir.

1.4. Nəticə

Cəmiyyətin bütün sferalarının qloballaşması, kiberməkanın formalaşması qanuna riayət edən vətəndaşlarla yanaşı, hüquq pozucuları üçün də asan üsullarla pozuntuların törədilməsi üçün imkanlar açır. Müasir dövrün ən aktual problemlərindən olan "kibertəhlükələr"lə mübarizə dünya miqyasında aparılır. Sərhədləri bilinməyən bir məkanda cinayətkarın axtarılması son dərəcə çətin olduğu üçün həm milli səviyyədə, həm də beynəlxalq səviyyədə kibermühitdə törədilən cinayətlərə "həssaslıqla" yanaşılmalıdır. Hətta, onu deyə bilərik ki, kibercinayətlər ənənəvi üsulla törədilən cinayətlə müqayisədə daha ağır nəticələrə səbəb ola bilir. Bu baxımdan, kibertəhlükələrin qarşısının alınması üzrə əməkdaşlıq prinsipi rəhbər tutulmalıdır. Bu, iki istiqamətdə aparılsa, daha operativ nəticələr əldə etmək olar: dövlətlərin əməkdaşlığı – beynəlxalq səviyyədə və vətəndaşla dövlət orqanlarının əməkdaşlığı – milli səviyyədə.

ƏDƏBİYYAT

1. Əliyev Ə.İ., Rzayeva G.A., İbrahimova A.N., Məhərrəmov B.A., Məmmədrzalı Ş.S. İnformasiya hüququ. Dərslik. Bakı: Nurlar, 2019, 448 s.
2. Creation of a global culture of cybersecurity: resolution / United Nations General Assembly (UNGA) Resolution 57/239, 31 January 2003. https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/unga-creation-global-culture-cybersecurity
3. Darrel C. Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. // Michigan Telecommunications and Technology Law Review, 1998, Volume 4, Issue 1, p. 69-103.
4. Dorothy J. Glancy. The invention of the right to privacy. // Arizona Law Review, 1979, Volume 21 (1), http://law.scu.edu/wp-content/uploads/Privacy.pdf
5. Dutfield G. Global intellectual property law: commentary and materials / Graham Dutfield [and others]. Northampton, MA: Edward Elgar Pub., 2005, pp. 238-252.
6. Fiordalisi E. The Tangled Web: Cross-Border Conflicts of Copyright Law in the Age of Internet Sharing. // Loyola University Chicago International Law Review, 2015, Vol. 12, İssue 2, pp. 197-213.
7. Gibson W. Burning chrome. Canada, 1982. http://project.cyberpunk.ru/lib/burning_chrome/
8. Gibson W. Neuromancer. First edition, 1984, 271 p.
9. National information society policy: A template. Developed by The Information For All Programme of UNESCO. Paris November 2009, 143 p.
10. Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech". / Adopted on 30 October 1997 by Committee of Ministers of Council of Europe. https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-97-20-of-the-committee-of-

ministers-to-member-states-on-hate-speech-?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/
11. Richard R. Bartle. Designing Virtual Worlds. New Riders, 2003, 741 p.
12. Samuel D. Warren, Louis D. Brandeis. The Right to Privacy. // Harvard Law Review, 1890, Vol. 4, No. 5, p. 193-220.
13. W.Lambert Gardiner. Virtual Reality/Cyberspace: Challenges to Communication Studies. // Canadian Journal of Communication, 1993, Vol 18 (3),http://www.cjc-online.ca/index.php/journal/article/view/762/668
14. William L.Prosser. Privacy. // California Law Review, 1960, Volume 48 (3), p. 383-423.
15. Рассолов И.М. Право и Интернет: Теоретические проблемы. Москва: Норма, 2009, 383 с.
16. Телешина Н.Н. Виртуальная пространства как новая юридическая конструкция: к постановке проблемы. // Юридическая техника, 2013, №7 (Ч.2), с. 740-747.
17. Туликов А. Интеллектуальная собственность в киберпространстве: правообладатели и общество готовы к диалогу. // Интеллектуальная собственность в киберпространстве: Сборник аналитических материалов проекта “Право и общество в цифровую эпоху”. МОО ВПП ЮНЕСКО “Информация для всех”. Составитель: Евгений Альтовский, 2006, с. 9-12.
18. http://virtualaz.org/
19. http://www.dictionary.com/browse/virtual-environment
20. http://www.virtualkarabakh.az/index.php?lang=3
21. https://www.eff.org/cyberspace-independence

ВИРТУАЛЬНОЕ ПРОСТРАНСТВО, КИБЕР УГРОЗЫ И ЗАЩИТА ПРАВ ЧЕЛОВЕКА

Г.Ф.РЗАЕВА

РЕЗЮМЕ

Изменение и развитие мировоззрения в современном обществе также оказывает влияние на незаконное поведение. Поскольку традиционные методы не соответствуют требованиям времени, ИКТ все чаще используются в качестве нового метода и инструмента для нарушения прав человека и совершения различных преступлений. Это также требует усиления борьбы с киберпреступностью. В статье выдвинуты предложения и рекомендации по разработке механизмов защиты прав человека, которые нарушаются киберпреступностью в глобальном информационном обществе.

Ключевые слова: глобальное информационное общество, киберпространство, киберпреступность, свобода выражения мнений, право на личную жизнь, права интеллектуальной собственности, информационная политика.

VIRTUAL SPACE, CYBER THREATS AND PROTECTION OF HUMAN RIGHTS

G.A.RZAYEVA

SUMMARY

Changing and developing world outlook in modern society also has an impact on illegal behavior. As traditional methods do not meet the requirements of the time, ICTs are increasingly being used as a new method and tool for violating human rights and committing different offences. This also requires strengthening the fight against cybercrimes. In the article were put forward suggestions and recommendations for the development of human rights protection mechanisms that have been violated by cybercrimes in the global information society.

Keywords: global information society, cyberspace, cybercrime, freedom of expression, right to personal privacy, intellectual property rights, information policy.