Kibertəhlükəsizliyin Təmin Olunmasında Kibercinayətkarlıqla Mübarizə: Hüquqi Problemlər və Qanunvericiliyin Təkmilləşdirilməsi Perspektivləri

Cavid Mirzəzadə
Dövlət Təhlükəsizliyi Xidməti, Bakı, Azərbaycan
mirzezadec2002@gmail.com

Xülasə **- Məqalədə kibercinayətkarlıqla mübarizənin əhəmiyyəti araşdırılmış, qloballaşan dünyanın İKT-dən artan asılılığı təhlil edilmiş, beynəlxalq təşkilatların kibertəhlükəsizliyin qorunması istiqamətindəki tövsiyələri, o cümlədən Azərbaycan Respublikasının kibercinayətkarlıqla mübarizə sahəsində qoşulduğu beynəlxalq müqavilələrin tələbləri nəzərdən keçirilmişdir. Kibercinayətkarlığın transmilli və qlobal xarakteri nəzərə alınmaqla milli qanunvericilikdə kibercinayət və kiberməkan məfhumlarının hüquqi definisiyasının müəyyən edilməsi, cinayət və sahəvi qanunvericiliyin bəzi müddəalarının təkmilləşdirilməsi, habelə prosessual sahənin, rəqəmsal sübutların hüquqi statusunun yeni çağırışlara uyğunlaşdırılması ilə əlaqədar təkliflər irəli sürülmüşdür.**

Açar sözlər – kibertəhlükəsizlik; kibercinayətlər; cinayət məsuliyyət; universal yurisdiksiya; rəqəmsal sübutlar.

I. Giriş

Qloballaşan dünyada informasiya-kommunikasiya texnologiyalarının (İKT) sürətli inkişaf tendensiyası informasiya cəmiyyətində müxtəlif risklərin meydana gəlməsinə səbəb olmaqla informasiya təhlükəsizliyinin təmin olunmasını dövlət siyasətinin mühüm tərkib hissəsinə çevirmişdir. Təsadüfi deyil ki, Azərbaycan Respublikasının informasiya məkanının müasir təhdidlərdən qorunması milli təhlükəsizliyin əsas istiqamətlərindən biri kimi bəyan edilmişdir [1]. Bu da öz növbəsində normativ hüquqi bazanın təkmilləşdirilməsini və müasir beynəlxalq standartlara uyğunlaşdırılmasını zərurətə çevirmişdir.

2025-ci ilin məlumatına əsasən, dünya əhalisinin 74 faizi internetdən istifadə etmişdir. 2024-cü ildə bu göstərici 71 faiz təşkil etmişdir. Başqa sözlə, bir il ərzində internet istifadəçilərinin sayı artaraq 5,8 milyarddan 6 milyard nəfərə çatmışdır ki, bu da dünyada illik artım tempinin bir qədər yüksələrək, 2,9 faizdən 3,3 faizə çatdığının göstəricisidir. İnkişaf etmiş dövlətlərdə əhalinin 94 faizi, Müstəqil Dövlətlər Birliyinə (MDB) üzv ölkələrdə isə 88-93 faizi internetdən istifadə edir [2]. Müvafiq statistik göstəricilər cəmiyyətlərin ciddi şəkildə rəqəmsal transformasiyasını sübut etməklə bərabər, əksər insan fəaliyyətlərinin onlayn şəkildə həyata keçirildiyini göstərir.

Şübhəsiz ki, mövcud vəziyyət elmi-texniki tərəqqinin mühüm nailiyyətlərinə əsaslanır. Lakin unutmaq olmaz ki, elm və texnologiyanın sürətli inkişafı hər nə qədər müsbət xarakterə malik olsa da, inkişafın nəticələrindən sui-istifadə halları da bir o qədər mənfi ictimai təhlükə doğuran nəticələrə yol aça bilər. Belə ki, İKT-nin inkişafı yeni hüquq sahələri ilə yanaşı, həm yeni cinayət növlərini, həm də ənənəvi cinayətlərin fərqli törədilmə üsullarını ortaya çıxarmışdır. Beləliklə, gündəlik həyatımızı əhəmiyyətli dərəcədə asanlaşdıran texnologiya və internet, digər tərəfdən yeni hüquqi tənzimləmələri zəruri edən bir problemə çevrilmişdir. Bu hal insan hüquq və azadlıqları sahəsində təməl prinsip və müddəalardan kənara çıxmamaq şərtilə yeni yanaşmaların tətbiq edilməsini labüd edir.

Hüquq nə qədər konservativ xarakter daşısa da, o, rəqəmsal transformasiya şəraitində cəmiyyətin bütün strukturunun ciddi dəyişikliklərə məruz qaldığı bir vaxtda dəyişən şərait və daim yenilənən ictimai münasibətlər nöqteyi-nəzərdən mövcud tələbatlara cavab verməlidir. Dünyanın rəqəmsal infrastrukturdan asılılığı artdıqca, kibertəhlükəsizliyin təmin olunması istiqamətində kibercinayətkarlıqla mübarizə məsələləri ön plana çıxır. Bu sahədə beynəlxalq əməkdaşlığı hədəfləyən Avropa Şurasının (bundan sonra – AŞ) 23 noyabr 2001-ci il tarixli “Kibercinayətkarlıq haqqında” (Budapeşt Konvensiyası) və Birləşmiş Millətlər Təşkilatının (bundan sonra – BMT) 24 dekabr 2024-cü il tarixli “Kibercinayətkarlığa qarşı” (Hanoy Konvensiyası) Konvensiyalarının mühüm əhəmiyyəti vardır. Azərbaycan Respublikası hər iki Konvensiyanın iştirakçısı olmaqla bərabər, Hanoy Konvensiyasını ilk ratifikasiya etmiş dövlətlərdən biridir.

Nəzərə almaq lazımdır ki, artıq bir sıra hüquqi anlayışların qanunda müasir anlamda təsbit edilməsinə və cəmiyyətin baş verən rəqəmsal transformasiyası, kibercinayətlərin artması və digər cinayətlərin rəqəmsal izlərinin sübuti əhəmiyyət qazanması tendensiyasına uyğunlaşdırılmasına zərurət yaranmışdır. Hazırkı tədqiqatın məqsədi mövcud hüquqi tənzimetmənin təhlil edilməsindən və ictimai münasibətlərin yenilənən təbiətinə uyğun olaraq kibertəhlükəsizliyin və informasiya cəmiyyətinin qorunması üçün qanunvericiliyin təkmilləşdirilməsi yönündə təkliflərin irəli sürülməsindən ibarətdir.

DOI: 10.25045/forensic.gov.2026.91

II. Kibertəhlükəsizliyin Təmin Edilməsi: Kibercinayətkarlığa Qarşı Mübarizənin Çətinlikləri

Kibertəhlükəsizlik və kibercinayətkarlıq geniş yayılmış və daim inkişaf edən kibertəhdidlər, rəqəmsal infrastrukturdan artan asılılıq fonunda şəxsiyyət, cəmiyyət və dövlətin təhlükəsizliyi üzərində əhəmiyyətli təsirə malik olması baxımından ciddi araşdırma tələb edən mövzulardır. Qeyd etdiyimiz kimi, kibertəhlükəsizliyin təmin olunmasında kibercinayətlərə qarşı mübarizə xüsusi əhəmiyyətə malikdir. BMT Baş Assambleyası tərəfindən kibertəhlükəsizliklə bağlı 2000-ci il 55/63 saylı "İnformasiya texnologiyalarından cinayət məqsədilə sui-istifadəyə qarşı mübarizə", 2001-ci il 56/121 saylı "İnformasiya texnologiyalarından cinayət məqsədilə sui-istifadəyə qarşı mübarizə", 2002-ci il 57/239 saylı "Kibertəhlükəsizlik üzrə qlobal mədəniyyətin yaradılması", 2003-cü il 58/199 saylı "Kibertəhlükəsizlik üzrə qlobal mədəniyyətin yaradılması və kritik informasiya infrastrukturlarının qorunması" və 2009-cu il 64/211 saylı "Kibertəhlükəsizlik üzrə qlobal mədəniyyətin yaradılması və kritik informasiya infrastrukturlarının qorunması sahəsində milli səylərin qiymətləndirilməsi" adlı qətnamələr qəbul edilmişdir.

Əvvəlki qətnamələrdən fərqli olaraq, Baş Assambleyanın 21 dekabr 2009-cu il tarixli 64/211 saylı qətnaməsində kibertəhlükəsizliyin təmin olunmasında kibercinayətkarlıqla mübarizənin əhəmiyyəti xüsusi vurğulanmış, sürətlə inkişaf edən İKT-dən asılılığın artması nəticəsində köhnələn və ya aktual olmayan hüquqi səlahiyyətlərin nəzərdən keçirilməsi və onların regional və beynəlxalq müqavilələrdən, razılaşmalardan və presedentlərdən istifadə edilməklə yenilənməsi, habelə kibercinayətkarlığın istintaqı və təqibi üçün dövlətlərin zəruri qanunvericiliyinin olub-olmadığının müəyyən edilməsi vəzifə kimi qarşıya qoyulmuşdur [3].

Kibertəhlükəsizlik İKT-nin davamlı inkişafında mühüm rol oynayır. Kibertəhlükəsizliyin gücləndirilməsi və kritik informasiya infrastrukturunun qorunması hər bir dövlətin təhlükəsizliyi və iqtisadi rifahı üçün vacibdir. Məhz kibercinayətlərin qarşısının alınması kibertəhlükəsizlik və kritik informasiya infrastrukturunun qorunması strategiyasının ayrılmaz tərkib hissəsi kimi çıxış edir. Bu strategiya milli səviyyədə İKT-dən sui-istifadə etməklə törədilən cinayətlərlə mübarizə aparılması üçün zəruri qanunların qəbulunu və kritik informasiya infrastrukturu obyektlərinin bütövlüyünə təsir göstərməyə yönəlmiş fəaliyyətlərin qarşısını almağı, beynəlxalq səviyyədə isə müvafiq istiqamətdə dövlətlərarası əməkdaşlığı və koordinasiyanı nəzərdə tutur.

Kibertəhlükəsizlik məsələsinin yaratdığı hüquqi, texniki və institusional çətinliklər qlobal xarakter daşıdığından, həmin çətinliklərin həll edilməsi beynəlxalq əməkdaşlıq çərçivəsində həyata keçirilən strategiyanın ortaya qoyulmasını labüd edir. Kibertəhlükəsizlik strategiyasının hazırlanması və həyata keçirilməsi kibercinayətkarlığa qarşı mübarizədə zəruri amildir. Bu baxımdan "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər üçün Strategiyası" müstəsna əhəmiyyətə malikdir.

Qeyd etmək lazımdır ki, kibertəhlükəsizliyin qorunmasında kibercinayətkarlıqla mübarizə zəruri olduğu qədər də problematik xarakterə malikdir. Fikrimizcə, bu istiqamətdə mövcud çətinliklərin və onların həlli yollarının bir neçə istiqamətdə qruplaşdırılması mümkündür.

Birincisi, qanunvericiliyimizdə və ratifikasiya etdiyimiz beynəlxalq sənədlərdə kibercinayət, kiberməkan və süni intellekt kimi terminlərin normativ hüquqi anlayışlarının mövcud olmaması, cinayət hüququ nəzəriyyəsində isə alimlər arasında mövzu ətrafında konsensusa gəlinməməsi nəzəriyyə və təcrübəni ciddi çətinliklərlə üzləşdirir. Həm Budapeşt, həm də Hanoy Konvensiyalarında kibercinayət termininin hüquqi tərifi təsbit edilməmişdir.

"Cinayətlərin qarşısının alınması və cinayətkarlıqla mübarizə üzrə" BMT-nin X konqresində isə kibercinayətlərin dar və geniş mənada iki növü fərqləndirilmişdir. Dar mənada kibercinayət (kompüter cinayəti) anlayışı elektron əməliyyatlar vasitəsilə törədilən və kompüter sistemlərinin, habelə onlar tərəfindən emal edilən məlumatların təhlükəsizliyini hədəf alan hər hansı qeyri-qanuni hərəkət və ya hərəkətsizliyi əhatə edir. Geniş mənada kibercinayət (kompüterlə əlaqəli cinayət) anlayışı isə kompüter sistemi və ya kompüter şəbəkəsi vasitəsilə və ya onunla əlaqədar törədilən hər hansı hərəkət və ya hərəkətsizliyi ifadə edir; buraya məlumatların qanunsuz saxlanılması, təqdim edilməsi və ya yayılması kimi cinayətlər də daxildir.

Geniş yayılmış təriflərdən birinə görə kibercinayət – kompüterlərin və ya şəbəkələrin cinayət fəaliyyətində alət, hədəf və ya mühit kimi istifadə olunduğu hər hansı fəaliyyətdir [4]. Bu fikirlə razılaşmaq çətindir. Əgər kompüter geniş mənada cinayətin hədəfi kimi seçilmişdirsə, bu kibercinayət olmaya da bilər. Məsələn, kompüter avadanlığının fiziki olaraq məhv edilməsi cinayət tərkibinin zəruri əlamətləri mövcud olduqda mülkiyyət əleyhinə cinayət kimi tövsif edilməlidir. Yaxud kompüter avadanlığından alət kimi istifadə edərək, başqa şəxsə fiziki xəsarət yetirilməsi müvafiq hallardan asılı olaraq həyat və ya sağlamlıq əleyhinə olan cinayət kimi tövsif edilə bilər.

"Kiber" ifadəsi bilavasitə kibernetika elminin predmetidir. Kibernetika isə idarə sistemləri, üsul və vasitələri haqqında elm sahəsidir [5]. Yunan dilindən tərcümədə hərfi mənası "idarə etmək məharəti" deməkdir. Oksford izahlı lüğətində nəzərdə tutulan "kiber" sözü dilimizə "informasiya texnologiyalarına, internet şəbəkəsinə və virtual mühitə aid olan" kimi tərcümə olunur.

Kibercinayətlərin kiberməkanda törədilməsi bu cinayətlərin zəruri ünsürüdür. Cinayət hüququ nəzəriyyəsində "kiber xarakterli cinayətlər" anlayışından da istifadə olunur və bu termin kibercinayət məfhumundan fərqləndirilir [6]. Hesab edirik ki, kiberməkanda törədilən cinayətlərin bu cür fərqləndirilməsinə zərurət yoxdur. Ona görə ki, kiberməkanda törədilən bütün cinayətlər kibercinayətdir. Eyni üsul və eyni məkanda törədilən cinayətlərin fərqli hüquqi statusla təmin olunması onların qarşısının alınması və nəticələrinin aradan qaldırılmasında, eləcə də dövlətlərarası əməkdaşlığın həyata keçirilməsində mövcud hüquqi imkanlardan eyni cür yararlanmağa imkan verməyəcəkdir. Kiberməkan istənilən kibercinayət tərkibinin zəruri əlamətidir. İstər İKT, istərsə də İKT ilə əlaqəli cinayətlər kiberməkanda törədilir. Bu nöqteyi-nəzərdən kibercinayət dedikdə, kiberməkanda İKT-dən istifadə etməklə və ya İKT-yə qarşı törədilən istənilən cinayət başa düşülməlidir. Məsələn, BMT Konvensiyasının 13-cü maddəsində İKT sistemi ilə əlaqəli oğurluq və ya dələduzluq

əməllərinin kriminallaşdırılması üzv dövlətlərin vəzifəsi kimi müəyyən olunmuşdur [7]. Bununla da, İKT vasitəsilə törədilən oğurluq və ya dələduzluq kibercinayətlər kateqoriyasına aid edilmişdir. Eyni qaydada AŞ Konvensiyasının 8-ci maddəsi də kompüter texnologiyalarından istifadə etməklə törədilən dələduzluq əməlinin kriminallaşdırılması üçün zəruri qanunvericilik və digər tədbirlərin görülməsini tərəflərin üzərinə qoymuşdur [8]. Bu baxımdan, "İKT səviyyəsində törədilən və insan hüquqlarını kobud şəkildə pozan hər bir cinayət kibercinayətdir" fikri xüsusi maraq doğurur [9].

Qeyd edilənlərlə yanaşı, kibercinayətlərin iki istiqamətdə qruplaşdırılmasını mümkün hesab edirik: İKT cinayətləri və İKT ilə əlaqəli cinayətlər. Bu baxımdan AŞ Konvensiyasının 3 və 4-cü yarımfəsillərində nəzərdə tutulan müvafiq olaraq “məlumatların məzmunu ilə bağlı cinayətlər” və “müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər” də İKT ilə əlaqəli cinayətdir [8]. Hesab edirik ki, həmin əməllərin ayrıca yarımfəsillərdə qruplaşdırılması tərəflərin qəsd obyektinin daha ciddi mühafizə altına alınmasını təmin etmək məqsədindən irəli gəlir.

“Kiberməkan – insanların, proqram təminatının və internetdəki xidmətlərin texnoloji cihazlar və onlara qoşulmuş şəbəkələr vasitəsilə qarşılıqlı əlaqəsi nəticəsində yaranan, fiziki formada mövcud olmayan mürəkkəb mühit kimi nəzərdən keçirilir [10].

İkincisi, kibercinayətlər nisbətən yeni növ cinayətlər kateqoriyasına aid olduğundan, bəzən hüquq-mühafizə orqanları bu sahədə zəruri biliklərə malik olmaya bilər. Sözsüz ki, hüquqi bilikləri formalaşdırmaq və ya təkmil varianta gətirmək normativ hüquqi bazanın təkmilləşdirilməsindən əhəmiyyətli dərəcədə asılıdır. Ona görə də bu funksiyanın qanunverici tərəfindən həyata keçirildiyini desək, yanılmarıq. Bu xüsusda təkliflərimizi tədqiqatın davamında irəli sürmüşük. Lakin bu tip cinayətlərin xarakteri zəruri hüquqi biliklərlə yanaşı, hüquq-mühafizə orqanları əməkdaşlarının minimum texniki biliklərə yiyələnməsini də şərtləndirir.

Üçüncüsü, transmilli xarakterə malik kibercinayətlərlə müəyyən ərazi yurisdiksiyaları daxilində mübarizənin aparılması onun səmərəliliyini məhdudlaşdırır [11]. Kiberməkan zamana və fiziki məkana xas məhdudiyyətlərə malik olmayan sərhədsiz mühitdir. Onun vasitəsilə törədilən cinayətlər çox asanlıqla dövlət sərhədlərini aşmağa və geniş spektri əhatə etməyə qadirdir. Bu isə dövlətlərin suveren bərabərliyi prinsipinə xələl gətirmədən yurisdiksiya problemlərinin həll olunmasını labüd edir.

Azərbaycan Respublikası Cinayət Məcəlləsinin (bundan sonra – CM) 12.3-cü maddəsi universal yurisdiksiya prinsipinin əsaslarını müəyyən edir [12]. Maddənin mətnində “kibercinayətlər” termini konkret olaraq təsbit olunmasa da, “cəzalandırılması Azərbaycan Respublikasının tərəfdar çıxdığı beynəlxalq müqavilələrdən irəli gələn digər cinayətlər” ifadəsi həmin kateqoriya cinayətləri də ehtiva etməkdədir. Çünki kibercinayətlərin kriminallaşdırılması dövlətin tərəfdar çıxdığı beynəlxalq müqavilələrin, yəni AŞ və BMT konvensiyalarının tələbidir. Bu baxımdan, kibercinayət törətmiş şəxsin hansı dövlətin vətəndaşı olmasından və cinayəti hansı ölkənin ərazisində törətməsindən asılı olmayaraq istənilən dövlətin milli qanunvericiliyi əsasında cinayət məsuliyyətinə cəlb edilməli və cəzalandırılmalıdır. Burada sual doğuran məqam isə CM-in XXX fəslində nəzərdə tutulmayan kiberməkanda törədilən cinayətlərə həmin maddənin qüvvəsinin şamil olunub-olunmaması məsələsidir. Konvensiyaların mətnlərinin sistemli və ardıcıl təhlili belə bir nəticəyə gəlməyə imkan verir ki, həmin cinayətlər də kibercinayət kimi qiymətləndirilməli və universal yurisdiksiya prinsipinin təsir dairəsinə düşməlidir.

Dördüncüsü, kibercinayətlərin aşkar edilməsi ehtimalı ənənəvi cinayətlərə nisbətən xeyli aşağıdır. Həqiqətən də, bu cinayətlərin törədildiyi vasitə və sistem böyük həcmdə texniki xarakter daşıyır və daim dəyişir; internetdən anonim istifadə imkanlarının mövcudluğu səbəbindən cinayətkarların müəyyən edilməsi imkanı bəzən çox məhdud olur. Bundan əlavə, informasiya sistemləri haqqında kifayət qədər biliyi olmayan şəxslər çox vaxt baş verən vəziyyətin fərqinə varmadan cinayətin qurbanına çevrilir [13].

Beşincisi, kibercinayətlərlə mübarizənin səmərəliliyi və effektivliyi dövlətlərarası əməkdaşlığın gücləndirilməsi sayəsində mümkündür. Ona görə də hüquq sistemlərinin və milli qanunvericiliklərin unifikasiyası gücləndirilməlidir. BMT Konvensiyası bu istiqamətdə hüquqi imkanlar təqdim edir. Konvensiyanın 64-cü maddəsinə əsasən, Konvensiyaya istənilən dövlət, həmçinin üzv dövlətlərindən ən azı biri bu Konvensiyanın tərəfi olan regional iqtisadi inteqrasiya təşkilatı qoşula bilər [7].

Bu fikirlə razıyıq ki, “kibercinayətlərə qarşı mübarizə ya qlobal olmalıdır, ya da heç bir mənası yoxdur” [14]. Çünki hətta bir neçə dövlət belə bu mübarizəyə qoşulmazsa, “jurisdiction shopping” (“yurisdiksiya seçimi” və ya “əlverişli yurisdiksiya axtarışı”) adlanan hal baş verəcək və kibercinayətkarlar bu cinayətlər üçün qanunvericiliyində ən az cəza nəzərdə tutan və ya digər dövlətlərlə hüquqi yardım haqqında müqavilələri olmayan dövlətləri müəyyən edərək, fəaliyyətlərini orada davam etdirəcəklər [13].

III. Qanunvericiliyin Təkmilləşdirilməsi Perspektivləri

Hesab edirik ki, milli qanunvericiliyin bir neçə istiqamətdə nəzərdən keçirilməsi, o cümlədən əlavə və dəyişikliklərin edilməsi labüddür.

03 aprel 1998-ci il tarixli “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikası Qanununun əsas anlayışları müəyyən edən 1-ci maddəsində [15] yuxarıdakı məzmunda kibercinayət və kiberməkan anlayışlarının təsbit edilməsi mütləqdir. Hazırda kibercinayətin definisiyasının mövcud olmaması bu kateqoriyaya daxil olan cinayətlərin dairəsinin qanunvericilik səviyyəsində müəyyənləşdirilməsinə imkan vermir. Bu isə bəzi hallarda cinayət təqibi orqanlarını və məhkəməni hüquq normalarının tətbiqində qeyri-müəyyən vəziyyətə sala bilər.

CM-in Ümumi hissəsinin müddəalarının təkmilləşdirilməsi kibercinayətkarlıqla mübarizədə zəruri addımlardan biridir. Müasir dövrdə cinayət qanunvericiliyinin təkmilləşdirilməsi perspektivləri kriminallaşdırma və dekriminallaşdırma proseslərinin elmi nəzəriyyə və məhkəmə təcrübəsi əsasında həyata keçirilməsi, cinayət qanunvericiliyinin sistemliyinin qorunması, cinayət məsuliyyətinin diferensiasiyası səviyyəsinin

daha da yüksəldilməsi, sanksiyaların vahid prinsiplər əsasında sistemli şəkildə yenidən qurulması, qanunvericilikdə mövcud olan boşluq və ziddiyyətlərin aradan qaldırılması, hüquqi texnikanın inkişafından əhəmiyyətli dərəcədə asılıdır [16].

Qeyd etdiyimiz kimi CM-in 12.3-cü maddəsi universal yurisdiksiya prinsipini müəyyən edir. Nəzərə almaq lazımdır ki, cinayət qanunvericiliyinin analogiya üzrə tətbiqi qanunla qadağan olunsa da, maddələrin genişləndirici təfsirinə münasibətdə bunu deyə bilmərik. Yuxarıda ifadə etdiyimiz mövqe ilə müvafiq maddəni genişləndirici şəkildə şərh edərək, universal yurisdiksiyanın kibercinayətlərə də şamil olunduğunu bildirdik. Bununla belə, məhkəmə təcrübəsinin vahidliyinin təmin olunması üçün konkret şəkildə "kibercinayətlər" termininin 12.3-cü maddəyə əlavə edilməsini təklif edirik. Lakin bu baş versə də, kibercinayət məfhumunun dəqiq sərhədlərinin qanunla müəyyənləşdirilməməsi bizi belə bir sual qarşısında qoyacaqdır: İKT vasitəsilə şəxsiyyət, mülkiyyət, dövlət hakimiyyəti və s. əleyhinə törədilmiş cinayətlərə universal yurisdiksiya prinsipi tətbiq oluna bilərmi?

Kibərməkanda törədilən bütün cinayətləri kibercinayət kimi qiymətləndirdiyimizdən artıq nəzəri cəhətdən göstərilən suala cavab vermişik. Lakin hüquq-mühafizə orqanlarının vahid və birmənalı nəticəyə gəlməsi üçün qanunvericinin bu məsələyə münasibət bildirməsi şərtdir. Bir daha vurğulamağı vacib hesab edirik ki, eyni üsul və eyni məkanda törədilən cinayətlərin fərqli hüquqi statuslara tabe edilməsi onların bir qisminə münasibətdə universal yurisdiksiya və bu kimi digər mühüm əhəmiyyətə malik hüquqi imkanların tətbiqindən dövlətləri məhrum etməklə bərabər, kibercinayətkarlığa qarşı mübarizədə dövlətlərarası əməkdaşlıq məsələlərini çətinə salacaqdır. Bu baxımdan istər CM-in XXX fəslində nəzərdə tutulmuş cinayətlər, istərsə də kiberüsulla və kibərməkanda törədilən digər cinayətlər kibercinayət hüquqi statusu ilə təmin olunmalıdır.

Məlum olduğu kimi, əksər cinayətlərin kibərməkanda törədilməsi mümkündür. Bu cinayətkarların sərhədsiz məkanın imkanlarından istifadə etməklə daha asan yolla öz niyyətlərinə çatmaq imkanının olması deməkdir. Qeyd edilən hal mübarizənin yalnız milli deyil, beynəlxalq səviyyədə əməkdaşlıq çərçivəsində həyata keçirilməsini tələb edir. Biz bu əməkdaşlığa daha münbit şərait yaratmaq üçün CM-in 12.3-cü maddəsinə kibərməkanda törədilməsi imkanı olan bütün cinayətləri daxil edə bilmərik, lakin həmin məkanda törədilə biləcək bütün cinayətləri müvafiq maddədə kibercinayət adı altında göstərə bilərik. Nəzərə alınmalıdır ki, müəlliflərin "kiber xarakterli cinayət" və ya "kiberləşmə əlamətinə malik cinayət" [6] adlandırdıqları kibərməkanda törədilməsi imkanı olan cinayətlər öz ictimai təhlükəliliyinin xarakteri və dərəcəsi baxımından CM-in XXX fəslində göstərilən əməllərdən qat-qat ağır ola bilər. Bu istiqamət üzrə ilk növbədə kibercinayətin qəti anlayışı qanunvericilik səviyyəsində təsbit edilməli, bununla yanaşı, CM-in 12.3-cü maddəsinə "kibercinayətlər" termini əlavə edilməlidir.

CM-in 20-ci maddəsi cinayət məsuliyyətinə cəlb etməyə imkan verən yaş həddini müəyyən edir. Qanunvericinin mövqeyinə görə xüsusi subyekt tərəfindən törədilməsi halları istisna olmaqla, kibercinayətlərə görə cinayət məsuliyyətinə cəlb etmə yaşı 16-dır [12]. Əvvəlki tədqiqatlarımızda cinayət məsuliyyətinin minimum yaş həddi anlayışına münasibət bildirərək, onu şəxsin psixi, fizioloji və intellektual yetkinliyə çatması ilə əlaqələndirmişik [17]. Ümumtəhsil müəssisələrində 1-ci sinifdən etibarən "informatika" adlı dərsliyin tədris edildiyi hamıya məlumdur. Bu ona dəlalət edir ki, ibtidai təhsili başa vurmuş şəxs artıq İKT barəsində kifayət qədər biliklərə yiyələnmiş olur. Xüsusilə də, müxtəlif ölkələrin təcrübəsində 10-16 yaş arası yetkinlik yaşına çatmayanlar içərisində kibercinayətlərin törədilməsi halları müşahidə edilir [18].

Cinayət məsuliyyəti yaşını təyin edərkən qanunverici bu yaşa qədər insanın öz ictimai təhlükəli hərəkətlərinin (hərəkətsizliyinin) mahiyyətindən və onların qadağan edilməsindən xəbərdar olmaq üçün kifayət qədər inkişaf səviyyəsinə çatması ehtimalından çıxış edir [19]. Bu baxımdan qanunvericinin hazırkı mövqeyi ilə razılaşmaq çətindir. Qeyd edilən çatışmazlığın iki istiqamətdə həll edilməsini mümkün sayırıq: CM-in 20.2-ci maddəsində cinayət törədənədək 14 yaşına çatmış şəxsin cinayət məsuliyyətinə cəlb edilə biləcəyi cinayətlərin siyahısına kibercinayətlər də əlavə olunmalıdır və ya CM-ə aşağıdakı məzmunda 20.3-cü maddə əlavə olunmalıdır: Cinayət törədənədək 12 yaşı tamam olmuş şəxs öz əməlinin (hərəkət və ya hərəkətsizliyinin) ictimai təhlükəliliyinin faktiki xarakterini dərk etmək və onu idarə edə bilmək qabiliyyətinə malikdirsə, həmin şəxs barəsində tərbiyəvi xarakterli məcburi tədbirlər tətbiq oluna bilər.

İkinci həll variantını daha məqbul hesab edirik. Bu yalnız kibercinayətlər deyil, eyni zamanda digər cinayətlər baxımından da geniş mənada cəzasızlığın yolverilməzliyi prinsipini təmin edəcəkdir. Belə ki, CM-in 84-cü maddəsi cinayət törədərkən on dörd yaşı tamam olmuş, lakin on səkkiz yaşına çatmayan şəxsləri yetkinlik yaşına çatmayan hesab edib, yalnız həmin şəxslərə münasibətdə cəza və ya tərbiyəvi xarakterli məcburi tədbirlərin tətbiq edilməsinin mümkünlüyünü müəyyən edərək, on dörd yaşına çatmayan şəxslər cinayət törətdikdə onlara tərbiyəvi xarakterli məcburi tədbirlər tətbiq etmək imkanından məhkəməni məhrum edir. Tərbiyəvi xarakterli məcburi tədbirlər cinayət məsuliyyətinin məzmununa daxil olmadığından [20], belə dəyişikliyin edilməsi qanunvericinin humanist mövqeyinə kölgə salmayacaqdır. Fikrimizcə, humanizm prinsipi öz təzahürünü qanunun sözlərindən daha çox, ədalət mühakiməsinin realizəsində və tətbiq edilən islah təsir tədbirlərinin xarakterində tapmalıdır. Humanizmin təminatçısı qanunvericidən ziyadə hüquq-mühafizə orqanları və məhkəmələrdir.

Müvafiq dəyişiklik beynəlxalq standartlara da tamamilə cavab verəcəkdir. Belə ki, Uşaq Hüquqları Komitəsi ümumi şərhlərində dövlətlərə cinayət məsuliyyətinə cəlb etmə yaşının on iki yaşa çatdırılmasını tövsiyə edir. Biz isə on iki yaşın cinayət məsuliyyətinin minimum yaş həddi kimi deyil, tərbiyəvi xarakterli məcburi tədbirlərin tətbiq edilməsi üçün ən aşağı yaş həddi olaraq qəbul edilməsini təklif edirik. Nəzərə almaq lazımdır ki, bir çox inkişaf etmiş ölkələrdə cinayət məsuliyyətinin minimum yaş həddi olduqca aşağıdır. Belə ki, cinayət məsuliyyətinə cəlb etmə Fransada 13 [21], Niderland [22] və Şotlandiyada [23] 12, Yeni Zelandiya [24], İsveçrə [25], İrlandiya [26] və İngiltərədə [27, 28] 10 yaşdan etibarən başlayır.

CM-in Xüsusi hissəsinin müddəalarının təkmilləşdirilməsi də Ümumi hissənin normalarının təkmilləşdirilməsi qədər mühüm əhəmiyyət kəsb edir. Əvvəla, XXX fəslin

“Kibercinayətlər” adlandırılması Azərbaycan Respublikasının qanunvericilik texnikasına ziddir. 2012-ci il dəyişikliklərinə qədər mövcud olmuş redaksiyada müvafiq fəslin “Kompüter informasiyası sahəsində cinayətlər” adlandırılmasını daha uğurlu yanaşma hesab edirik. Qeyd etmək lazımdır ki, Rusiya Federasiyası CM-in analoji cinayətlərə görə məsuliyyət müəyyən edən 28-ci fəsli “Kompüter informasiyası sahəsində cinayətlər [29], Türkiyə Cümhuriyyəti Türk Cəza Qanununun 3-cü bölməsinin 10-cu fəsli isə “İnformasiya texnologiyaları (bilişim) sahəsində cinayətlər” [30] adlandırılır. Bunun səbəbi qanunvericilər tərəfindən cinayət qanunlarının Xüsusi hissələrinin strukturlaşdırılmasında qəsd obyektinə uyğun bölgü aparılması, bölmələrin adlandırılmasının cinsi, fəsillərin adlandırılmasının növ, maddələrin adlandırılmasının isə bilavasitə obyektə görə həyata keçirilməsidir. Buna görə də fəslin adlandırılmasında cinayətin adından deyil, onun qəsd etdiyi ictimai münasibətlərin konkret qrupunun adından istifadə olunmalıdır. Fikrimizcə, XXX fəslin "Kibertəhlükəsizlik əleyhinə cinayətlər" adlandırılması daha məqsədəuyğundur. Bunun səbəbi həmin fəsildə nəzərdə tutulmuş cinayətlərin növ obyektinin kibertəhlükəsizliyi təmin edən ictimai münasibətlər olmasıdır. Həm də nəzərə alınmalıdır ki, kibercinayətlərin hamısı XXX fəsildə təsbit olunmayıb. Bu, qəsd obyektinin fərqli olmasından irəli gəlir. Məsələn, kiberoğurluq əməlinin (CM-in 177.2.3-1-ci maddəsi) əsas bilavasitə obyekti mülkiyyətin toxunulmazlığını təmin edən ictimai münasibətlər, əlavə bilavasitə obyekti isə kibertəhlükəsizliyi təmin edən ictimai münasibətlərdir. Ona görə də müvafiq cinayət tərkibi mülkiyyət əleyhinə olan cinayətlər fəslində yerləşdirilmişdir. Çünki bu tip cinayətlər, o cümlədən oğurluq əməli həmişə kibermәkanda törədilmir.

CM-in Xüsusi hissəsinin XXX fəslində nəzərdə tutulmuş kibercinayətlər böyük ictimai təhlükə törətməyən və az ağır cinayətlər kateqoriyasına aid edilmişdir. Hətta formal tərkibli cinayət olan İKT sisteminə qanunsuz daxil olma (CM-in 271-ci maddəsi) maddi tərkibli cinayət olan İKT sisteminə və ya elektron verilənlərə qanunsuz müdaxilə (CM-in 273-cü maddəsi) ilə analoji sanksiyaya malikdir. Artıq cinayət hüququ nəzəriyyəsində kibercinayətlərə görə təyin edilən cəzaların cinayətə mütənasib olmamasının mübahisələndirilməsi halları az deyil [11]. Qeyd edilənləri nəzərə alaraq, kibercinayətlərə görə sanksiyaların vahid prinsiplər əsasında qurulması, xüsusilə də əməlin kritik informasiya infrastrukturu obyektlərinə münasibətdə törədildiyi hallara görə məsuliyyət müəyyən edən normalarda cəzaların sərtləşdirilməsi qanunverici tərəfindən təmin edilməlidir.

CM-in 273-1-ci maddəsinin adı ilə dispozisiyası arasında uyğunsuzluq mövcuddur. Belə ki, maddənin adı kibercinayətlərin törədilməsi üçün hazırlanmış vasitələrin dövriyyəsidir. Lakin maddənin mətnində yalnız 271-273-cü maddələrdə nəzərdə tutulmuş əməllər kibercinayət kimi qiymətləndirilmişdir. Buradan belə bir nəticə hasil olunur ki, kiberoğurluğun və ya kiberdələduzluğun, habelə digər cinayətlərin kibermәkanda törədilməsi məqsədilə hazırlanmış və ya uyğunlaşdırılmış hər hansı qurğu və ya kompüter proqramının istehsalı, həmin cinayətlərin törədilməsi məqsədi ilə idxalı, istifadə üçün əldə olunması, saxlanılması, satışı, yayılması və ya əldə edilməsinə digər formalarda şərait yaradılması, əhəmiyyətli zərər vurduqda həmin əməllər kibercinayət sayılmadığından CM-in 273-1-ci maddəsi üzrə məsuliyyət yaranmayacaqdır. Bu mövqeni haqlı hesab etməyərək müvafiq maddənin dispozisiyasına konkret maddələrin göstərilməsi əvəzinə “kibercinayətlər” ifadəsinin daxil edilməsini daha düzgün hesab edirik.

30 aprel 2013-cü il tarixli “Azərbaycan Respublikasının Cinayət Məcəlləsində dəyişiklik edilməsi haqqında” Azərbaycan Respublikasının Qanunu ilə oğurluq əməlinin “elektron məlumat daşıyıcılarından, yaxud informasiya texnologiyalarından istifadə edilməklə törədilməsi”nin ağırlaşdırıcı tərkib əlaməti kimi CM-ə əlavə edilməsini müsbət qiymətləndirir, bu tendensiyanın davamlı olmasını, yəni şəxsiyyət, mülkiyyət, dövlət hakimiyyəti və s. əleyhinə olan kibermәkan vasitəsilə törədilmə imkanına malik digər cinayət tərkiblərini nəzərdə tutan maddələrə də ağırlaşdırıcı tərkib əlaməti kimi cinayətin İKT-dən istifadə edilməklə törədilməsinin daxil edilməsini arzuolunan hesab edirik. Bu hal tövsif məsələlərində də müsbət istiqamətdə dəyişikliklərin baş verməsinə imkan yaradacaqdır. Məsələn, dələduzluğa görə məsuliyyət müəyyən edən CM-in 178-ci maddəsində əməlin kibermәkan vasitəsilə, yəni İKT-dən istifadə etməklə törədilməsini nəzərdə tutan tərkib əlaməti mövcud deyil. BMT Konvensiyasının “İKT sistemi ilə bağlı oğurluq və ya dələduzluq” adlanan 13-cü maddəsinə əsasən, hər bir iştirakçı Dövlət qəsdən və qanunsuz olaraq törədildiyi hallarda şəxsin özü və ya başqa bir şəxs üçün pul və ya digər əmlak əldə etmək kimi dələduzluq və ya digər vicdansız niyyətlə aşağıdakı yollarla başqa bir şəxsə əmlak zərərinin vurulmasına səbəb olmasını öz daxili qanunvericiliyinə əsasən cinayət əməli kimi müəyyən etmək üçün zəruri qanunvericilik və digər tədbirləri görür:

(a) Elektron verilənlərin hər hansı formada daxil edilməsi, dəyişdirilməsi, silinməsi və ya gizlədilməsi;

(b) İKT sisteminin fəaliyyətinə hər hansı müdaxilə;

(c) İKT sistemi vasitəsilə faktiki hallarla bağlı aldadıcı məlumat vermək və bunun nəticəsində şəxsin normal halda etməyəcəyi hərəkəti etməsinə və ya edəcəyi hərəkəti etməməsinə səbəb olmaq. Deməli, elektron verilənlərin daxil edilməsi, dəyişdirilməsi, silinməsi və ya gizlədilməsi, yaxud İKT sisteminə müdaxilə etməklə törədilən dələduzluq əməli cinayətlərin məcmusu qaydasında, yəni CM-in 178 və 273-cü maddələrinin müvafiq hissələri ilə tövsif olunmalıdır.

CM-in 171-1.1-ci maddəsi uşaq pornoqrafiyasını yayma, reklam etmə, satma, başqasına vermə, göndərmə, təklif etmə, əldə edilməsinə şərait yaratma, yaxud yaymaq və ya reklam etmək məqsədilə hazırlama, əldə etmə və ya saxlamağa görə məsuliyyət müəyyən edir. Fikrimizcə, müvafiq normanın dispozisiyasına BMT Konvensiyasının 14-cü maddəsinə uyğun olaraq uşaq pornoqrafiyasının sifariş edilməsi və idarə olunması (uşaq pornoqrafiyasına nəzarət) əməllərinin də daxil edilməsi məqsədəuyğundur. Eyni zamanda qeyd etdiyimiz əməllər də daxil olmaqla 171-1.1-ci maddədə nəzərdə tutulmuş əməllərin İKT-dən istifadə edilməklə törədilməsinin ağırlaşdırıcı tərkib əlaməti kimi CM-in 171-1.2-ci maddəsinə əlavə edilməsini təklif edirik. Bundan başqa, Konvensiyanın 14-cü maddəsində iştirakçı dövlətlərə eyni əməllərin maliyyələşdirilməsi cinayətinin kriminallaşdırılması da tövsiyə edilmişdir. Hesab

edirik ki, CM-ə 171-1.1-ci maddədə nəzərdə tutulmuş əməllərin maliyyələşdirilməsinə görə cinayət məsuliyyəti müəyyən edən 171-1.1-1-ci maddə əlavə edilməlidir.

Bununla yanaşı, CM-ə AŞ Konvensiyasının 10-cu maddəsinə müvafiq olaraq, müəlliflik hüquqlarını və ya əlaqəli hüquqları İKT-dən istifadə etməklə pozmağa görə cinayət məsuliyyəti nəzərdə tutan 165.2.3-cü maddənin əlavə edilməsini təklif edirik.

Maddi normaların təkmilləşdirilməsi ilə yanaşı, prosessual hüquq normalarının da nəzərdən keçirilməsini məqsədəuyğun hesab edirik. BMT Konvensiyasının 23-cü maddəsinin 1-ci bəndinə əsasən, hər bir iştirakçı Dövlət konvensiyanın 4-cü fəslində nəzərdə tutulan səlahiyyət və prosedurların konkret cinayətlərin araşdırılması və ya icraatı məqsədilə həyata keçirilməsi üçün zəruri olan qanunvericilik və digər tədbirləri qəbul etməlidir. Həmin maddənin 2-ci bəndinə görə Konvensiyada başqa hal nəzərdə tutulmayıbsa, hər bir iştirakçı Dövlət 1-ci bənddə göstərilən səlahiyyət və prosedurları aşağıdakılara tətbiq etməlidir:

(a) Bu Konvensiyaya uyğun olaraq müəyyən edilmiş cinayət əməllərinə;

(b) İKT sistemi vasitəsilə törədilən digər cinayət əməllərinə;

(c) Hər hansı cinayət əməli üzrə elektron formada sübutların toplanmasına.

Konvensiyanın trafik verilənlərinin real-vaxt rejimində toplanmasını nəzərdə tutan 29-cu maddəsinin 1-ci bəndinə əsasən, hər bir iştirakçı Dövlət öz səlahiyyətli orqanlarına aşağıdakı səlahiyyətləri vermək üçün zəruri qanunvericilik və digər tədbirləri qəbul etməlidir:

(a) Həmin dövlətin ərazisində texniki vasitələrin tətbiqi ilə məlumatları toplamaq və ya qeydə almaq; və

(b) Xidmət provayderini, onun mövcud texniki imkanları daxilində:

(c) həmin dövlətin ərazisində texniki vasitələrdən istifadə etməklə məlumatları toplamağa və ya qeydə almağa məcbur etmək; və ya

(d) səlahiyyətli orqanları məlumatların toplanması və ya qeydə alınmasında əməkdaşlıq etməyə və yardım göstərməyə məcbur etmək;

Beləliklə, İKT sistemi vasitəsilə ötürülən və həmin ərazidə baş verən müəyyən edilmiş kommunikasiya ilə bağlı trafik verilənlərinin real-vaxt rejimində toplanması və ya qeydə alınması təmin edilir.

Konvensiyanın 2-ci maddəsinin (c) yarımbəndinə uyğun olaraq "trafik verilənləri" - İKT sistemi vasitəsilə həyata keçirilən kommunikasiya ilə bağlı olan, həmin sistem tərəfindən yaradılan və kommunikasiya zəncirinin bir hissəsi olan, rabitənin mənşəyini, təyinatını, marşrutunu, vaxtını, tarixini, ölçüsünü, müddətini və ya istifadə olunan xidmətin növünü göstərən istənilən elektron verilən deməkdir.

Konvensiyanın məzmun verilənlərinin ələ keçirilməsini nəzərdə tutan 30-cu maddəsi ciddi cinayət əməlləri ilə bağlı 29-cu maddədə nəzərdə tutulmuş analoji qanunvericilik və digər tədbirlərin görülməsi vəzifəsini təsbit edir. Konvensiyanın 2-ci maddəsinin (d) yarımbəndinə uyğun olaraq "məzmun verilənləri" — abunəçi məlumatları və ya trafik verilənləri istisna olmaqla, İKT sistemi vasitəsilə ötürülən məlumatların mahiyyəti ilə bağlı olan istənilən elektron verilən deməkdir. Buraya şəkillər, mətn mesajları, səs mesajları, audioyazılar və videoyazılar da daxildir.

Konvensiyanın 2-ci maddəsinin (h) yarımbəndinə əsasən, ciddi cinayət – törədilməsinə görə ən azı dörd il azadlıqdan məhrumetmə cəzası və ya daha ağır cəza nəzərdə tutulan cinayətdir. Həmin maddənin (e) yarımbəndinə görə xidmət provayderi aşağıdakı funksiyalardan birini və ya hər ikisini həyata keçirən istənilən dövlət və ya özəl qurum deməkdir:

(i) Öz xidmətinin istifadəçilərini İKT sistemi vasitəsilə kommunikasiya imkanı ilə təmin edən; və ya

(ii) Belə bir kommunikasiya xidməti və ya həmin xidmətin istifadəçiləri adından elektron verilənləri emal edən və ya saxlayan.

Konvensiyanın 23-cü maddəsinin 3-cü bəndinin (a) yarımbəndinə görə hər bir iştirakçı Dövlət bu Konvensiyanın 29-cu maddəsində nəzərdə tutulan tədbirlərin tətbiqini yalnız öz qeyd-şərtində göstərilən cinayət və ya cinayət kateqoriyalarına şamil etmək hüququnu özündə saxlaya bilər, bir şərtlə ki, həmin cinayətlərin və ya cinayət kateqoriyalarının əhatə dairəsi 30-cu maddədə nəzərdə tutulan tədbirlərin tətbiq olunduğu cinayətlərin əhatə dairəsindən daha dar olmasın. Hər bir iştirakçı Dövlət bu cür qeyd-şərtin mümkün qədər məhdudlaşdırılmasını nəzərdən keçirməlidir ki, 29-cu maddədə nəzərdə tutulan tədbirlər ən geniş şəkildə tətbiq olunsun [7].

Təqdirəlayiq haldır ki, "Azərbaycan Respublikasının Cinayət Məcəlləsində və Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsində dəyişiklik edilməsi haqqında" Azərbaycan Respublikasının 03 mart 2026-cı il tarixli 373-VIIQD nömrəli Qanununda BMT Konvensiyasının yuxarıda göstərilən normaları nəzərə alınmışdır. Elektron formada sübutların hüquqi statusunun müəyyən edilməsi, elektron verilənlər, habelə abunəçi məlumatları, trafik və məzmun verilənləri terminlərinin CPM-in əsas anlayışları təsbit edən 7-ci maddəsinə daxil edilməsi və sübutetmə prosesi qaydalarının yeni sübut növünə ardıcıl uyğunlaşdırılması [31] qanunvericiliyin əhəmiyyətli yeniliyi kimi qiymətləndirilməlidir.

Cinayət-Prosessual hüquq nəzəriyyəsində təklif olunan konsepsiyalardan biri də sübutların yazılı (kağız) formada rəsmiləşdirilməsindən imtina olunmasıdır [32]. Əgər sübutetmə prosesinin modernləşdirilməsinin birinci istiqaməti elektron formada sübutların əldə edilməsi və rəsmiləşdirilməsinin qanunvericilik səviyyəsində təsbit olunmasıdırsa, ikinci istiqamət artıq elektron informasiyanın müstəntiqin kağız protokollarından və elektron daşıyıcılardan ayrılmasıdır. Bu elektron sənəd dövriyyəsinin formalaşmasına əməli surətdə şərait yaradacaqdır.

09 mart 2004-cü il tarixli "Elektron imza və elektron sənəd haqqında" Azərbaycan Respublikası Qanununun 1.1.16-cı maddəsi elektron sənəd dövriyyəsini informasiya sistemində elektron sənədin nizamlanmış hərəkəti ilə bağlı informasiya prosesləri, həmin Qanunun 1.1.15-ci maddəsi isə elektron

sənədi elektron formada, o cümlədən mətn, səs, görüntü və ya audio-görüntü formasında saxlanılan kontent kimi müəyyən etmişdir [33]. Əldə edilmiş rəqəmsal sübutların cinayət işinin materiallarına elektron formada əlavə edilməsi və saxlanılmasının mümkünlüyü istintaq orqanlarının işini əhəmiyyətli dərəcədə yüngülləşdirəcəkdir. Bir sıra hallarda bank sistemlərində, mobil rabitə şəbəkələrində, kommunikasiya xidmətlərində, ani mesajlaşma platformalarında, habelə internet şəbəkəsində, videomüşahidə sistemlərində, istifadəçilərin "ağıllı cihazlarında" və digər fərdi qurğularında cinayət işi üzrə əhəmiyyət kəsb edən böyük həcmdə informasiya toplanılması ehtimalı olduğundan, bu mənbələrdən elektron sübutların götürülməsi prioritet xarakter daşıyır. Elektron məlumatların bu cihaz və sistemlərdən elektron üsulla götürülməsi və işə əlavə edilməsi onların əldə olunması müddətini kəskin şəkildə azaldacaqdır. Digər tərəfdən elektron sübutların istintaq protokolunda qismən təsvir etməklə deyil, bütöv və dəyişdirilməmiş formada cinayət işinin materiallarına əlavə olunması istintaq orqanlarına daha çox informativ dəyərə malik olan orijinal məlumatı əldə etməyə imkan verəcəkdir.

Anglo-sakson hüquq sistemində "ən yaxşı sübut qaydası" (best evidence rule) mövcuddur ki, buna əsasən sübut xarakterli hər bir informasiyada faktın ilkin mənbəyi (orijinal forması) əsas əhəmiyyət daşıyır. ABŞ Federal Sübut Qaydalarının 1002-ci maddəsində qeyd edilir ki, məhkəməyə orijinal yazının təqdim edilməsi tələb olunur. Elektron verilənlərə münasibətdə isə onların yaradılması və saxlanmasının etibarlılığı, məlumatın bütövlüyünün yoxlanılması üsulu və onun yaradıcısının müəyyən edilməsi kimi adi tələblərin tətbiq edildiyi bildirilir. Elektron informasiyanın orijinalının araşdırılması əlavə olaraq "metaverilənlər"in (metadata) kriminalistik əhəmiyyətini üzə çıxarmağa imkan verir. Bu məlumatlar sənədin mənşəyini, müəllifini, yaradılma anından istintaq orqanları tərəfindən əldə olunana qədər edilən dəyişiklikləri müəyyən etməyə imkan yaradır və onun sübuti əhəmiyyətini artırır.

Nəticə

Beləliklə, kibercinayətkarlığa qarşı mübarizə kibertəhlükəsizliyin təmin olunmasında ilk addımlardan biri kimi qiymətləndirilməlidir. Ciddi rəqəmsal transformasiya şəraitində İKT-dən artan asılılıq yeni cinayət növləri ilə yanaşı, ənənəvi cinayətlərin yeni törədilmə üsullarını ortaya çıxarır. Bu nöqteyi-nəzərdən mövcud hüquqi anlayışların nəzərdən keçirilməsi və ənənəvi hüquqi səlahiyyətlərə yenidən nəzərdən keçirilməsi prioritet məsələlərdən biri kimi çıxış edir. Normativ hüquqi bazanın cəmiyyətin mövcud tələbatlarına və beynəlxalq standartlara uyğunlaşdırılması, dövlətlərarası əməkdaşlıq üçün unifikasiyanın təmin edilməsi, habelə beynəlxalq müqavilələrin tələblərinə riayət olunması kibercinayətkarlıqla mübarizəyə öz töhfəsini verəcəkdir.

Qeyd edilənləri nəzərə alaraq, milli qanunvericiliyin bəzi müddəalarının dəyişdirilməsi və əlavələrin edilməsi yönündə bir sıra təkliflərimizi irəli sürürük. Bu istiqamətdə dövlətlərarası əməkdaşlığın zəruri aləti olan universal yurisdiksiya prinsipinin təsir dairəsinə düşən cinayətlərin sırasına kibercinayətlərin də daxil edilməsini, kibercinayət və kibərməkan məfhumlarına qanunvericilik səviyyəsində konkret anlayış verilməsini, kibercinayətlərin dairəsinin dəqiqləşdirilməsini, CM-in Xüsusi hissəsində cinayət məsuliyyəti müəyyən edən müddəaların nəzərdən keçirilməsini və mümkün əlavələrin edilməsini, müstəntiqin saysız cildlərdən ibarət kağız materiallarından elektron sənəd dövriyyəsinə keçilməsini labüd sayırıq.

Nəticə olaraq, hüquq sistemi və qanunvericilik elə bir vəziyyətə gətirilməlidir ki, uzunmüddətli perspektivdə yenilənən ictimai münasibətləri tənzim etmək iqtidarında olsun. Artıq ənənəvi yanaşmalarla yeni çağırışlar arasında, ictimai münasibətlərin dinamikliyi ilə hüququn sabitliyi arasında optimal balans yaradılmalıdır.

Ədəbiyyat

[1] Azərbaycan Respublikası Prezidentinin Sərəncamı, "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023-2027-ci illər Strategiyası"nın təsdiq edilməsi haqqında, 2023. https://e-qanun.az/framework/55045.

[2] ITU, "Almost three-quarters of the population are online: Internet use – Statistics," 2025.

[3] United Nations General Assembly, "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures," 2009. https://documents.un.org/doc/undoc/gen/n09/474/49/pdf/n0947449.pdf.

[4] International Telecommunication Union, Understanding Cybercrime: Phenomena, Challenges and Legal Response. Geneva, Switzerland: ITU, 2012.

[5] Azərbaycan Dilinin İzahlı Lüğəti, II cild. Bakı: Şərq-Qərb, 2006.

[6] S. N. Rzayeva and V. A. Sadiqli, "Cinayətin kiber üsulla törədilməsi – cəzanı ağırlaşdıran hal kimi," Polis Akademiyasının Elmi Xəbərləri, no. 4 (36), p. 198, 2022.

[7] UNODC, "Birləşmiş Millətlər Təşkilatının 'Kibercinayətkarlığa qarşı' Konvensiyası," 2024. https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html.

[8] Avropa Şurası, "Kibercinayətkarlıq haqqında" Konvensiya, 2001. https://e-qanun.az/framework/18619.

[9] J. R. Agustina, "Book Review of Cyber Criminology: Exploring Internet Crimes and Criminal Behavior," International Journal of Cyber Criminology (IJCC), vol. 6, no. 2, pp. 1044-1048, Jul.–Dec. 2012.

[10] National Institute of Standards and Technology (NIST), "Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity," Draft Report, 2015.

[11] E. P. Balacanov, "Kibercinayətkarlıqla mübarizədə hüquqi tənzimetmənin və cinayət hüquqi normaların rolu və əhəmiyyəti," Azərbaycan Hüquq Jurnalı, no. 1, pp. 26-37, 2020.

[12] Azərbaycan Respublikasının Cinayət Məcəlləsi. Bakı: Hüquq Yayın Evi, 2025.

[13] M. Önak, "Avrupa Konseyi Siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği," https://dergipark.org.tr/en/download/article-file/814473.

[14] G. Esposito, "The Council of Europe Convention on Cyber-crime: A Revolutionary Instrument?," in Proceedings of the 2nd Asia Cyber Crime Summit, R. Broadhurst, Ed. Hong Kong: Centre for Criminology, University of Hong Kong, 2004.

[15] Azərbaycan Respublikasının Qanunu, "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında," 1998. https://e-qanun.az/framework/3525.

[16] C. C. Mirzəzadə, "Yaş həddi fiziki şəxsin cinayət məsuliyyətinin şərti kimi," Cinayət hüququnun aktual problemləri (Elmi məqalələr məcmuəsi), Ş. T. Səmədovanın ümumi redaktəsi ilə, Bakı: Mütərcim, 2022.

[17] Ş. T. Səmədova, "Azərbaycan Respublikasının Cinayət hüququ: Müasir dövrdə inkişaf perspektivləri," Cinayət hüququnun aktual problemləri (Elmi məqalələr məcmuəsi), Ş. T. Səmədovanın ümumi redaktəsi ilə, Bakı: Mütərcim, 2022.

[18] The Hacker News, "12-year-old Boy admits to hacking major

Government sites for aiding Anonymous Hackers,” 2013. https://thehackernews.com/2013/10/12-year-old-boy-admits-to-hacking-major_27.html?m=1.

[19] В. С. Комиссаров, Н. Е. Крылова, and И. М. Тяжкова, Ред., Уголовное право Российской Федерации. Общая часть: Учебник для вузов. Москва: Статут, 2012.

[20] F. Y. Səməndərov, Cinayət hüququ Ümumi hissə, Dərslik. Bakı: Hüquq Yayın Evi, 2018.

[21] Penal Code of France, 1994. https://www.unodc.org/cld/uploads/res/document/french_penal_code_html/french_penal_code.pdf.

[22] Criminal Procedure Code of the Netherlands, 1921. https://policehumanrightsresources.org/content/uploads/2016/08/Criminal-Procedure-Code-Netherlands-1921.pdf.

[23] Age of Criminal Responsibility Act 2019 (Scotland). https://www.legislation.gov.uk/asp/2019/7.

[24] Crimes Act 1961 (New Zealand). https://www.unodc.org/cld/uploads/res/document/nzl/1962/crimes_act_1961_html/New_Zealand_Crimes_Act.pdf.

[25] Swiss Criminal Code of 21 December 1937. https://www.unodc.org/uploads/icsant/documents/Legislation/Switzerland/311.0_Swiss_Criminal_Code_of_21_December_1937_English.pdf.

[26] Children Act 2001 (Ireland). https://www.irishstatutebook.ie/eli/2001/act/24/enacted/en/html.

[27] Children and Young Persons Act 1933 (UK). https://www.legislation.gov.uk/ukpga/Geo5/23-24/12/section/50.

[28] Criminal Law Act 1977 (UK). https://www.legislation.gov.uk/ukpga/1977/45.

[29] The Criminal Code of The Russian Federation, 1996. https://www.wto.org/english/thewto_e/acc_e/rus_e/wtaccrus58_leg_362/pdf.

[30] C. Ülgen, Türk Ceza Kanunu. İstanbul: Beta Yayın Evi, 2020.

[31] Azərbaycan Respublikasının Cinayət-Prosessual Məcəlləsi, 2000. https://e-qanun.az/framework/46950.

[32] А. А. Дмитриева and П. С. Пастухов, “Концепция электронного доказательства в уголовном судопроизводстве,” Journal of Digital Technologies and Law, vol. 1, no. 1, pp. 270-295, 2023. https://cyberleninka.ru/article/n/kontseptsiya-elektronnogo-dokazatelstva-v-ugolovnom-sudoproizvodstve/viewer.

[33] Azərbaycan Respublikasının Qanunu, “Elektron imza və elektron sənəd haqqında,” 2004. https://e-qanun.az/framework/5916.

Cybersecurity Enforcement in Combating Cybercrime: Legal Issues and Prospects for Improving Legislation

Cavid Mirzazade
State Security Service, Baku, Azerbaijan
mirzezadec2002@gmail.com

Abstract - The article examines the importance of combating cybercrime in ensuring cybersecurity, analyzes the increasing dependence of the globalized world on information and communication technologies, and reviews the recommendations of international organizations in the field of cybersecurity, including the requirements of international agreements to which the Republic of Azerbaijan is a party in the fight against cybercrime. Taking into account the transnational and global nature of cybercrime, proposals are put forward to define the legal concepts of cybercrime and cyberspace in national legislation, to improve certain provisions of criminal and sectoral legislation, and to adapt procedural law—particularly the legal status of digital evidence—to new challenges.

Keywords – cybersecurity; cybercrimes; criminal liability; universal jurisdiction; digital evidence.